Exploiting Digital Evidence Artefacts
Finding and joining digital dots

Brady, Owen Defries

Awarding institution:
King's College London

Exploiting Digital Evidence Artefacts

Finding and joining digital dots

Owen Brady

Supervisor: Dr Richard Overill

Department of Informatics
King's College London

This dissertation is submitted for the degree of
Doctor of Philosophy

King's College London April 2018

Acknowledgements

The process of researching and writing this thesis has taken eight years. In that time, many people have helped along the way but, in particular, I would like to thank: Lyn Goh for her support and time in reading countless versions of research papers; Michael Johnson for allowing me to bore him in the pub whilst explaining my ideas - and for his healthy scepticism; Ken O'Donnell for his continuous support and encouragement; Roddy Cook for educating me on the "Long Game" when investigating financial crime; and my brother Jon, whose erudite comments on early drafts of this thesis helped more than he may appreciate. My supervisor Richard Overill has been superb. Always giving just the right advice on navigating the academic system and turning around manuscript drafts with amazing speed. But finally, I would like to thank my wife, Rudi, and children - Meg, Cel and Siân. My apologies, in studying for this PhD at weekends and in the evenings, I haven't spent as much time with you as I should have - particularly in this last year. Rudi, thank you for your patience and support. I will now start on that long list of outstanding DIY jobs.

Abstract

As digital evidence becomes increasingly significant to criminal investigations, so does the importance of adopting the most effective approach to examining it. An ineffective examination can result in evidence not being identified. Even if evidence is noted, connections may not be made between the disparate values. This thesis proposes a new classification system to gauge, select and compare digital evidence from a variety of sources. It performs this using a type of model called an ontology. This is used to map the potential location of evidence on digital devices - applying a code to each piece that is identified. The codes are then used for selection of the artefacts that are most appropriate to enquiries based on the investigative Who, What, When, Where, How and Why questions. Any evidence with the same code can be compared. In applying this ontology it is demonstrated how investigations are made more effective, and the reliability of any recovered evidence can be more easily understood.

Table of contents

List of figures vii

List of tables ix

1 Introduction 1
- 1.1 Hypothesis . . . 3
- 1.2 Research questions . . . 4
- 1.3 Clarity of terminology . . . 4
- 1.4 Previously published material . . . 6
- 1.5 Structure of this thesis . . . 6

2 Setting the scene 8
- 2.1 What is a criminal investigation and how is it conducted? . . . 8
- 2.2 What is evidence? . . . 10
- 2.3 Forensics - terminology and use . . . 10
- 2.4 Traditional forensics and developments . . . 12
- 2.5 Factors influencing forensic examination . . . 16
- 2.6 Digital Evidence - the beauty and the beast . . . 19
- 2.7 Peripheral uses of Digital Evidence . . . 21
- 2.8 Current and developing challenges for Digital Evidence . . . 22
- 2.9 Tools and approaches that have advanced the field . . . 28
- 2.10 Previous research on digital evidence tools . . . 38
- 2.11 Digital evidence tools . . . 41
- 2.12 Conclusions . . . 47

3 Related Work 49
- 3.1 Introduction . . . 49
- 3.2 Terminology . . . 50
- 3.3 The contribution of models . . . 59
- 3.4 Selected ontologies indirectly related to Digital Evidence . . . 64
- 3.5 Digital Evidence ontologies - summary of findings . . . 70
- 3.6 Summary . . . 72

4 DESO - General Structure and Addressing Availability 75
4.1 Introduction . . . 75
4.2 Research methodology . . . 75
4.3 Alternative approaches that were not successful . . . 76
4.4 Introduction to the Digital Evidence Semantic Ontology (DESO) . . . 78
4.5 The Artefact Location class . . . 82

5 DESO - Addressing Selection, Correlation and Reliability 101
5.1 The Type Identifier class . . . 101
5.2 The Reference class . . . 118
5.3 Summary of DESO . . . 123

6 Comparative test application and evaluation of DESO 124
6.1 Introduction . . . 124
6.2 Investigation scenario . . . 124
6.3 Selection of monolithic tools . . . 125
6.4 Consideration of tool use . . . 125
6.5 Test - availability of artefacts . . . 126
6.6 Test - selection of artefacts . . . 127
6.7 Testing the correlation of artefacts . . . 134
6.8 Assessing the reliability of artefacts . . . 139
6.9 Summary of assistance provided by DESO . . . 140

7 Evaluation of DESO against objectives 143
7.1 Introduction . . . 143
7.2 Availability . . . 144
7.3 Selection of available artefacts . . . 146
7.4 Correlation of artefacts . . . 147
7.5 Reliance . . . 148
7.6 Summary . . . 149

8 Further work 150
8.1 Type Identification classes - How and Why . . . 150
8.2 Specification of artefact Location - a universal language . . . 150
8.3 Modification of existing ontologies . . . 151
8.4 Provenance ratings to assess weight of evidence . . . 151
8.5 DESO reporting to aid tool testing . . . 151
8.6 Fragments of data . . . 152
8.7 Expanding DESO's coverage . . . 152
8.8 Use of the dateAddedToDESO data property . . . 153

9 Summary and conclusions **154**
9.1 Summary of work 154
9.2 Conclusions 156
9.3 Contributions of the research 157
9.4 Identified limitations of the approach 160
9.5 Lesson learned - the obscurity of ontologies 162

References **163**

Appendix A Generation of test data **179**

Appendix B Table detailing Digital Evidence ontologies **180**

List of figures

2.1 The investigative Process . . . 9
2.2 The specialist / generalist trade-off . . . 11
2.3 The effects of increasing Digital Evidence volume . . . 24
2.4 The effects of increasing Digital Evidence variety . . . 26
2.5 The E-Discovery Reference Model (EDRM) . . . 35

3.1 An example taxonomy . . . 51
3.2 An example ontology . . . 53

4.1 File path represented as a class structure . . . 77
4.2 A representation of artefacts as classes . . . 79
4.3 The three classes of DESO . . . 80
4.4 The three DESO classes with two sample artefacts to show population . . . 83
4.5 Top-level structure of the Location class . . . 85
4.6 Location Class: Device Subclass . . . 88
4.7 Location Class: the addition of a sub-class for Solid State Devices . . . 89
4.8 Adding and rearranging classes . . . 89
4.9 Example Data Properties used in the Location Class . . . 91
4.10 The Data properties used in the Location Class to show position within a block . . . 92
4.11 The hierarchy of DESO's data properties . . . 94
4.12 Location Class: File System sub-class . . . 95
4.13 Location Class: Operating System Sub-class . . . 97
4.14 Location sub-class: Operating System Dependent Application files . . . 98
4.15 Location sub-class: illustration of Operating System . . . 100

5.1 Top level structure of the Identifier sub-class . . . 102
5.2 Identifier Class: the What sub-class . . . 105
5.3 The Friend of a Friend ontology . . . 106
5.4 Identifier Class: the Who sub-class . . . 108
5.5 Identifier Class: the Where sub-class . . . 109
5.6 Illustration of data as multiple Locations and Type Identifiers . . . 111
5.7 Illustrating the problems of time stamp interpretation . . . 113

5.8 Type Identifier: the When category 114
5.9 Using When Stage 1: iOS artefacts and DESO location 115
5.10 Using When Stage 2: assignment of Location to Type Identifier 116
5.11 Using When Stage 3: linking using “hasTimestamp” 117
5.12 Bibliographic Ontology classes and data properties 120
5.13 Top level Structure of the Reference Class 121
5.14 Object properties between the Location and Reference classes 122

6.1 The selection of artefacts for extraction 126
6.2 Two approaches to searching for artefact Type Identifiers 131
6.3 Axiom’s USB Device view 135
6.4 Axiom’s display of a parsed Windows 7 Jump List 135
6.5 Tools shown with differing reporting methods 137
6.6 DESO used for monolithic tool output 138
6.7 DESO as part of the investigative process 141

List of tables

1.1 Common Forensic Science Techniques And Their Uses 3

2.1 The Provenance Levels for Digital Evidence 29

4.1 Location - top level class structure 84

5.1 Exploring the application of 5WH to Digital Evidence 103

6.1 Common artefacts between a USB memory stick and Windows / OS X . . 132

Chapter 1

Introduction

As technology becomes further embedded into modern life it generates increasing amounts of digital traces. The traces, also known as "artefacts", shed light on how, when, where and by whom the technology was used. This information can become useful evidence in the investigation of criminal offences. This thesis describes a new approach for locating and exploiting these artefacts.

To understand why this fresh approach is required, it is useful to consider the perspective of a person trying to conduct an examination of a digital device to look for evidence. Before starting to look at any potential source, the following questions need to be considered:

- What records are available on this source?
- Of these records, which ones will assist my investigation and how do I use them?
- How do I know with certainty what these records represent?

The issues of volume and variety are commonly cited as the key problems of digital evidence. Volume, because of the increasing number of digital devices encountered in society which also have expanding storage capacities. Variety, because of the ever changing nature of technology and the difficulty in keeping pace with it.

But this thesis argues that these are aggravating factors not the root cause of the problems encountered with digital evidence. These instead are

- Availability;
- Selection;
- Correlation; and
- Reliance.

Availability

The first problem is knowing what data is available and, of this data, which of it is potentially useful? The distinction of the helpful data from the superfluous is dependent on knowing the description and location of potential evidential artefacts. The description is particularly important for, without it, how will any artefact be identified? Tools and methods can be built to handle extra volume - improving speed and efficiency - but they will be of little use without first identifying a target. This problem exists with any evidential source - even a piece of paper. Without knowing what you are looking for, how will you know when you have found it?

Selection

The second problem stems from the first - even if you have a complete set of descriptions of potentially useful artefacts how can those that assist a particular enquiry be sieved from the total set identified? Unless this is done then the examiner is not able to concentrate on those artefacts that assist an investigation and discard those that do not. This wastes resource.

Correlation

The third problem stems from the use of evidential artefacts. Whilst there are occasions where words on a page or in an email may prove useful in documenting a person's state of mind, a large part of any evidential examination is comparison - understanding whether one value matches another. Examples of physical evidence are shown in table 1.1. So this ability to compare the artefacts' values to see if they match is key to effective examination. The idea is to understand what can be compared and how to perform this comparison. This problem exists where there is any disparity between evidential sources but increasing variety compounds it.

Reliability

The fourth problem takes into account not just whether a particular value has been accurately copied and what it represents but also the reasoning for this representation. For example, a date and time is seen on a computer and labelled as the first time it was connected to a particular network. But what is the justification for saying this and is this assertion always accurate? For without this assurance, there is an uncertain provenance to the evidence. If this is carried through to a criminal trial it could lead to a miscarriage of justice where a person is wrongly convicted and sentenced to imprisonment.

At present, there is no central source of information to reference about the availability of artefacts, no system for selecting the artefact relevant to a particular case, no method for allowing easy comparison of artefact data and no method for documenting the provenance of an artefact and its representation. This leaves a gap which the approach outlined in this thesis aims to fill.

Table 1.1 (Based on material sourced from [100, p. 19]

Common forensic science techniques and their uses

Forensic Technique	What Does It Show?	Why is this useful?
Tool Marks - comparing the marks on an implement against those found, for example, on a window that was forced open	Can show a particular tool made a mark on a place or a person	Links a person found in possession of a tool with a crime scene
Ballistic striation marks - comparing the marks made by gun barrel on ammunition rounds against those found at a scene or in a body	That a particular firearm fired a round of ammunition	Links a person found in possession of a firearm to a shooting
Finger Marks - comparing finger mark impressions found at a crime scene to the finger prints of a person	Shows a particular person touched an object or other person	Links a person to a crime scene
DNA - comparing DNA traces found at a crime scene to those of a person	Can show a particular person was present at a place at some time	Demonstrates the presence of person at a place

1.1 Hypothesis

In consideration of the highlighted problems, the hypothesis being evaluated is that:

> **an ontology can improve the effective examination of digital evidence in large criminal cases.**

The research requirements for this evaluation are as follows:

- conduct a thorough examination of the issues that need to be addressed to see an improvement in examination;
- formulate an ontology to address these issues;
- test the ontology to assess its impact on existing tools and processes; and
- gauge which aspects of the approach are effective.

The first requirement - a thorough examination of the issues to be addressed - is detailed at Chapter 2. This gives rise to Research Questions for each of the identified four problems which any design and evaluation of an ontology must consider. As a primer, these are now detailed.

1.2 Research questions

Principal Question

- **RQ1:** Can a classification system be devised that allows for the documentation of digital evidence artefacts and facilitates their extraction and comparison?

Availability

- **RQ2:** How can this classification system allow for differing digital sources and rapid changes in technology?

Selection

- **RQ3:** Is it possible for this classification system to reduce the volume of digital evidence that requires examination?
- **RQ4:** Can this classification system allow for the selection of artefacts based on investigative criteria as opposed to technical ones?

Correlation

- **RQ5:** Can the classification system allow for successful comparison of artefacts irrespective of their source or originating format?
- **RQ6:** Can the classification system allow the use of any tools to process evidence?

Reliance

- **RQ7:** Can the classification system provide for the provenance of these artefacts to be established?

1.3 Clarity of terminology

There are a number of technical terms used in this thesis and, for clarity, these will now be outlined.

1.3.1 Digital Evidence

The term ‘Digital Evidence’ is discussed at length in section 2.6 but for the purposes of introducing the topic it represents, “Information stored or transmitted in binary form that may be relied upon in court.” [67, Pg 113]

1.3.2 Digital Forensics

The process by which this evidence comes to be collected and presented to a court of law is digital forensics - the term 'Forensic' means 'relating to or denoting the application of scientific methods and techniques to the investigation of crime / relating to courts of law.'[234]

It should be noted that the word 'forensic' is often used in the Information Technology field to mean any type of investigation - particularly regarding computer networks - but this use is not replicated in other areas of Forensic Science and is not intended for the purposes of this thesis.

There is a difference between the data that users explicitly create on devices – such as pictures and documents - and records that are created about the actual use of these devices - meta-data And it is these latter records that principally concern the fields of digital evidence and computer forensics.

As noted by Walden,[254]:

> investigators are generally more concerned with data generated by the technology itself, such as machine logs, than the content of the data that has been supplied to, and processed by, the technology. This so-called 'meta-data' describes and gives information about other data and will be generated by different elements within each of the computers and networks that process the content.

This thesis will also make this distinction between user-generated data, such as the documents, spreadsheets and emails, and system meta-data as earlier referenced by Walden - concentrating on the latter.

1.3.3 Artefact

The term "artefact" is used frequently in this dissertation. Dictionaries [47, 188] are relatively settled in defining the term as an object, made by a human, with some sort of cultural or historical interest. The term is widened - possibly abused - in the field of digital forensics to cover not only human actions but also those by machines as they interact. For example, the records left by one computer as it communicates with another.

When considering archaeological artefacts from a prior civilisation, it is not just, for example, a piece of pottery that is of interest but where it was found, its position and what else was found along side it.

Similarly, whilst all digital devices - by their very definition - use binary as a fundamental recording tool, a digital forensic artefact is more than this binary code. The way in which this code is interpreted as, for example, a photograph or document and the place in which it is stored on a device all go to the interpretation of what this binary means.

Finally, a short clarification on spelling. The commonly used version of the word in the United Kingdom (UK) is “artefact” whilst in the US, and possibly elsewhere, it is “artifact”. Since this dissertation is written in the UK, the first definition will be used unless directly quoting from a source that uses the alternate.

1.3.4 Ontologies

The term Ontology is described at length, later, in section 3.2.3. As a working definition, in the field of knowledge representation, an ontology is a means of describing a conceptual view of something - for example how animals can be categorised into different groups. Classes and sub-classes are used to provide a structure and members - “instances” - are placed within this structure.

Logical statements are made about these classes: one example would be the properties an instance must fulfil to be included in a particular sub-class - for example, a member of the “mammal” class must have the property “has sweat glands”. Another would be stating that if an instance was a member of one particular sub-classes then it cannot also be a member of another - as example a member of the “mammal” class cannot also be a member of the “reptile class”.

1.4 Previously published material

1. Addressing the Increasing Volume and Variety of Digital Evidence Using an Ontology. IEEE Joint Intelligence and Security Informatics Conference 2014 [34]

2. DESO: Addressing volume and variety in large-scale criminal cases. The International Journal of Digital Forensics and Incident Response, Volume 15 [35]

1.5 Structure of this thesis

Chapter 2 provides a background to the research. This covers the process of criminal investigation and then an introduction to evidence. Three current forensic disciplines are covered in depth: Fingerprints, Ballistics and DNA. This is to understand the factors that have influenced them and any lessons that could be learned from their development.

Digital Evidence is then introduced - what the term means and how this material is used in an investigation. After a consideration of some challenges posed by the increasing volume and variety of material, there is discussion on tools. This covers both the tools used to examine digital evidence and prior research on them.

The Chapter ends with a conclusion that some form of classification would assist the field of digital evidence. Research Questions are set.

Chapter 3 is focussed research on methods to classify and document digital evidence. After a discussion on terminology, the Chapter looks at Digital Evidence models before

considering ontologies. Both ontologies from within and outside the Digital Evidence field are considered. But none are found as a complete answer to address the Research Questions.

In Chapter 4 the Digital Evidence Semantic Ontology (DESO) is set out as an answer. First there is an overview of the ontology's structure before considering one of its classes: Location. This shows how artefacts can be documented and also how the structure for this documentation can be developed as technology advances.

Chapter 5 continues the description of DESO by introducing the remaining two classes: Type Identifier and Reference. These are used to select Digital Evidence artefacts, compare their data and assess their reliability.

Chapter 6 tests DESO by understanding how it can assist the use of common forensic tools when addressing a sample scenario. This application is evaluated in Chapter 7.

The lessons learned from this evaluation are brought forward to Chapter 8 which details further work.

Finally, Chapter 9 summarises the research then concludes by assessing both its contributions and limitations.

Chapter 2

Setting the scene

This chapter provides an introduction on topics relevant to digital evidence. It covers the following areas:

- A description of criminal investigations - the processes used to conduct them and the conditions that must be fulfilled;
- A description of "forensics" - first a clarification of terminology followed by the role it plays in criminal investigations. The field as a whole will first be discussed - not just digital evidence. This is because developments and challenges in other fields may be relevant to digital evidence;
- The specific field of digital evidence will then be introduced - first from a broad basis, including the various fora in which it is used - and then focussing on its use in criminal investigations. This first, brief, introduction to the arena is useful because it defines the problems addressed by this thesis;
- There is a then a description of previous attempts to mitigate and solve the described problems; and
- Finally, conclusions followed by a statement of the problem that will be addressed by the research and measures of success by which it should be judged.

2.1 What is a criminal investigation and how is it conducted?

A criminal investigation is "an effective search for material to bring an offender to justice" [70]. This can take a number of forms but, at its simplest, this is an enquiry into whether a crime has been committed and, if so, who could have committed it.

An investigation is, simply, a process followed to achieve the investigative objectives - as illustrated in Figure 2.1. As can be seen, the process is an iterative one which starts with

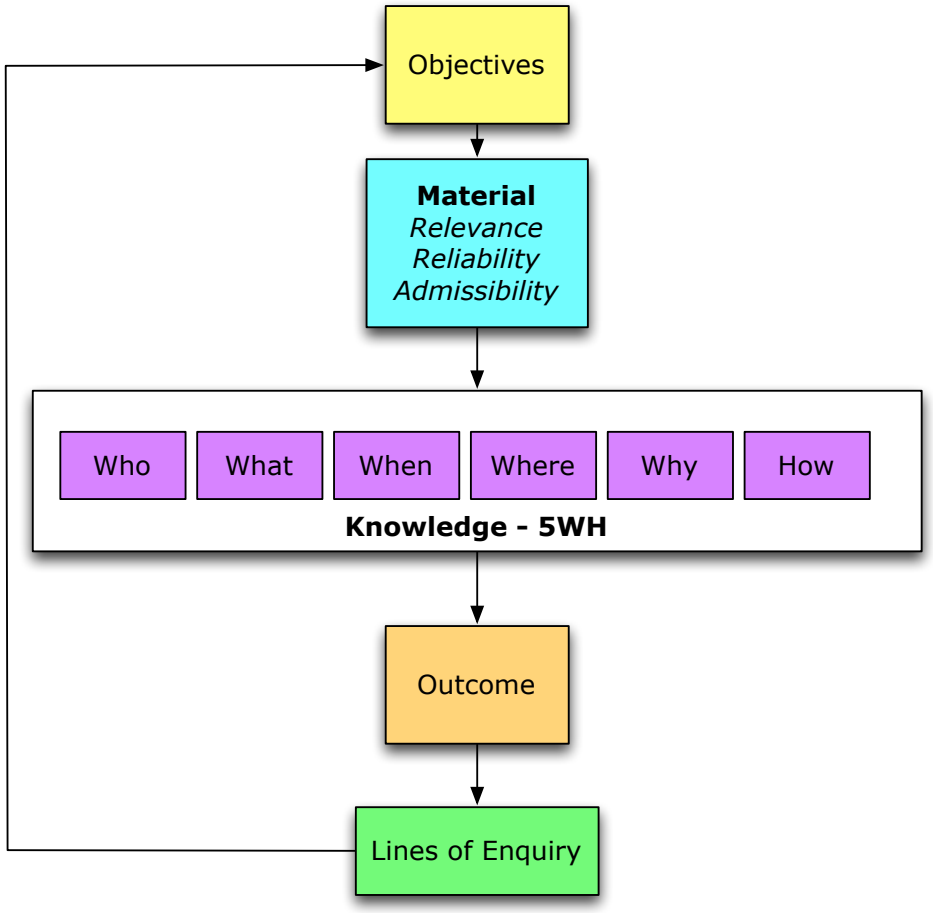

Fig. 2.1 The Investigative Process [70, p. 65]

the actual formation of the objectives. Knowledge is gained by the process of asking the simple questions: who, what, when, where, how and why? ("5WH") [70]. As questions are answered, the objectives may change.

For instance, if a person's dead body is found, the first investigative objective will always be *is this death suspicious*? In furtherance of this objective, the question to be asked is how did this person die? It could be simply that they died of natural causes such as a heart attack or they were suffering from terminal cancer. Enquiries with, for example, the Doctor treating the deceased could confirm this. An examination of the body and the scene may support this hypothesis.

But if there is any suspicion then it may become a criminal investigation and the next objective will be: *who played a part in this person's death*? Questions such as where the person was before they died, who this person met and the time that they died might be further investigated.

In a further investigative cycle the objective may be establishing the evidence that strengthens or weakens the case that a certain person committed this act. So the questions to be asked include: where was the suspect at the time of the person's death?

In each one of these iterative cycles, the answers to the 5WH questions may be garnered by making connections between various pieces of information. Examples are:

- Public transport records show the suspect alighting at a bus stop near the deceased's house at a pertinent time;
- a piece of paper containing the victim's handwriting is found on the suspect; and
- a cigarette containing the suspect's DNA was found at the victim's house.

For an investigation to be effective, these connections must be made and then enquiries conducted. Further, because the objectives can change over time, the investigator may have to review the available evidence on multiple occasions - the area of interest changes as knowledge increases.

An investigation is not a formally defined linear process where the end result, and the steps to achieve this result, can be predicted at the start. Instead it is iterative and modular and these modules are selected and adapted along the way. Any solution to the examination of digital evidence must be nimble in its ability to adapt to these changing needs of an investigation.

2.2 What is evidence?

The scope of evidence that can be admitted by a Court is rather wide - defined as: "for the purpose of determining the existence or non-existence of facts in issue" [151, p.21]. This includes oral evidence from witnesses, documentary evidence, which often includes digital material, and "things" - such as a knife used to stab a victim.

For evidence to be admitted in Court it must be "relevant" - making " the [facts in issue] more or less probable" [246]. In other words, if it can have some bearing on the facts being decided in the court case, it is relevant.

The collection and examination of non-oral evidence is often labelled as "forensics" and it is to this area that the thesis now turns. First, a discussion on terminology followed by consideration of the role that forensics plays in the criminal investigation process. Finally, there will be a brief inspection of non-digital forensic techniques as a foundation for the later discussion on digital evidence.

2.3 Forensics - terminology and use

Forensic science is science used for the purposes of the law. [136]

Whilst this is a relatively clear definition, it is worth briefly examining the terminology used in the forensics field - not only from a perspective of accuracy but also because it provides a useful window into the problems that are later seen with Digital Evidence.

Figure 2.2 illustrates the problem. At one side is effectively, the generalist investigators. These personnel will interview witnesses, process exhibits and / or examine crime scenes - collecting items for examination.

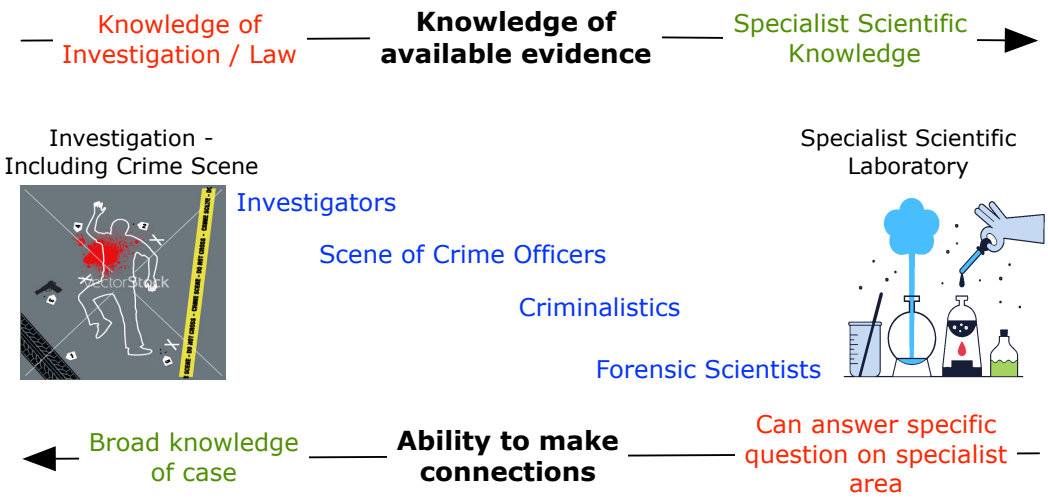

Fig. 2.2 Illustrating the balance between knowledge of the case and specialist knowledge of scientific techniques

At the other side are scientists who are relatively divorced from the investigation - they will have a detailed knowledge of their own specific area and of the appropriate standards and methodologies that must be applied when interpreting the results. In this respect they may even have their own terminology to describe their findings.

In between, there are roles across this spectrum as the range moves from knowledge of the case to knowledge of a specialist scientific area. [1]

There are problems that arise when this situation is viewed from two different perspectives: before examination (availability and selection of tests) and after (correlation of results).

2.3.1 Availability of evidence

The specialist scientist will have a detailed knowledge of the tests that could be performed in their specific area of expertise. Further, it has been argued [177] that the separation of the scientist from the investigation avoids the possibility of cognitive bias - being unduly influenced by a desire to help the investigator.

But, if this separation is to be effective, it relies on the investigator requesting the correct tests on the items submitted to the laboratory.

To date, no documented method has been identified for making the translation between investigative objectives and available tests.

[1] The term “criminalistics” is one used principally in the US and has a variety of meanings[46, 81] but broadly appears to be a synonym for forensic science.

2.3.2 Correlation of evidence

Analogous to the availability of evidence is correlation. Once the various tests have been conducted, how can the results be combined and compared to make the connections outlined at section 2.1? For instance, the handwriting on a note in the suspect's possession is compared to a specimen of writing that has been identified as being written by the victim.

If scientists are totally divorced from the investigation, and each other, Roux et al [212] warn about the creation of silos of knowledge. This leads to fragmentation because the findings from disparate experts are not correlated and effectively applied to the investigation. As evidence they note previous failures documented in a report on the "9-11" terrorist attack in the US [150]. This report noted how data from various sources were not integrated.

This does not mean there should be no specialists - or that they should be integrated in the investigation. Instead it argues that their specialist results should be capable of easy assimilation and comparison by investigators.

The point to be made is that if the field of forensic science was totally compiled of expert scientists conducting tests and then reporting them using field-specific terminology, it is left to the investigator to make sense of these results and understand their significance within the context of the investigation. This can lead to inaccuracy and missed evidential opportunities.

2.3.3 Summary of problem

In essence, the problem facing the forensics field is as follows:

- without sufficient expertise in a field there will be insufficient knowledge of all the tests that could be conducted;
- without sufficient expertise in a field, test results may be interpreted incorrectly;
- without sufficient knowledge of the investigation there will difficulty in knowing which tests will be most appropriate to advance enquiries; and
- if test results are not comparable across disciplines then valuable connections can be missed

This will become evident not just in the next section covering traditional forensic disciplines, but also digital evidence.

2.4 Traditional forensics and developments

It has been argued that the start of, what we would now call, "forensics" dated from the AD 700s when the Chinese used finger prints in the identification of documents and clay pots [141]. This section will not be a history of the field from this time but will draw

on a selection of the disciplines - some noted earlier in Table 1.1 - to understand how these fields operate and how they have developed. The intention is to understand whether anything can be learned and applied to the more recent field of digital evidence.

The forensic disciplines chosen are the examination of friction ridge skin analysis - also called "fingerprints", DNA and ballistics. The choice has been influenced by these disciplines still being in wide spread use - a point that will be covered at the end of this section.

2.4.1 Fingerprints

Fingerprint analysis is one of the longest used identification methods due, simply, to it being known for longer. Whilst finger prints are commonly viewed as a method of evidencing the presence of a particular person at a location, the criminal justice system is also heavily reliant on it for proving previous criminal convictions. The history is traced by the US Department of Justice's "Fingerprint Source Book" [171].

Finger prints have been used for identification since, as earlier reported, the AD 700s but the first recorded classification system for them was not until the late 1800s by Alphonse Bertillon [171, pg 5-4]. This was later discarded for being insufficiently distinctive and granular.

The next advance was work by Galton in 1892 where he discussed various classification approaches [103, chapter 5]. This included not just how to classify fingerprints but also their persistence, evidential weight and indexing. His findings were summarised: a "systematic, understandable, and applicable system of fingerprint classification had to be developed." [171, pg 5-6].

Differing classification systems were developed in various jurisdictions over the next century to allow comparison - the driver for change being the desire for Automated Fingerprint Identification Systems (AFIS) as the number of records increased. The AFIS scans any available fingerprints on a system and returns a set number of those that may match the fingerprints being assessed. The examiner can then review these and make a final confirmation.

The problem was that there was no standard amongst the AFIS vendors - reportedly due to budgetary and commercial competition factors. This caused problems both domestically and internationally in allowing an exchange of data.

Over time, however, standards were developed. In 1993 the American National Standards Institute [10] created a classification that was adopted by Interpol in 1996 - meaning that it was used by at least 181 countries outside the US [154, p.40]. The standard works on two levels: one, a protocol for the transmission of fingerprint images - essentially the raw data; and two, a vocabulary and transmission protocol for exchanging data about the features - or minutia - contained within the images. Over the years various revisions have been introduced with the latest published in 2016 [163].

The transmission of both the raw data and the features within it is not efficient - if just the features could be accurately defined and recorded then transmitting these alone without the raw data would reduce transmission time.

But the classification of fingerprints is not a straightforward process as they are biometrics - the measurement of a biological characteristic. Whilst a vocabulary for describing features can be agreed, the application of this vocabulary can vary amongst vendors [177, pg276]. The US National Institute for Standards and Technology (NIST) has approached this problem by developing a template for recording minutia and a testing programme, "Minex III" [170], against which various AFIS vendors can test the accuracy of their coding algorithms. Results are publicly available.

There are points that can be taken from the development of fingerprint standards:

- right from the start of fingerprint comparison, a classification system was required to index and compare them;
- as volume increased, this classification had to change to allow standardisation and machine reading; and
- standardisation was not a simple task - indeed taking many years - because of commercial as opposed to technical difficulties. Resolution came from central standard setting and testing by a government agency.

2.4.2 Ballistics

Valier [250] details a history of firearms examination - or ballistics - dating back to 1835 when Henry Goddard started to compare rifling in gun barrels against marks on discharged bullets.

Like fingerprints, ballistics has developed a classification system and this has allowed the creation of Integrated Ballistic Identification Systems (IBIS). Weapons can be classified by class characteristics such as: the diameter of the ammunition; the number of, and widths between, rifling marks - which are manufactured in the barrel to spin ammunition for accuracy; and whether the rifling twists to the left or right [244].

Individual weapons are distinguished by smaller marks - or stria - left on the surface of a bullet as it is propelled out of the firearm. The ability to individualise one firearm from another is formed from the manufacturing process where the tools made to manufacture the barrel will always be slightly different due to wear and tear. This means that a different combination of stria will be left by each weapon - and these can be seen on any discharged bullet.

Heard describes the examination of these stria as being a manual process which can only be performed by an experienced examiner. This is due to the need to not only note matching stria patterns but also discount those that do not. [129, pg. 182]. The process

is summarised: “A positive match between two sets of stria is one in which the extent of agreement exceeds that of the best accepted non - match. ”

The earlier mentioned IBIS are, effectively, image comparison engines - comparing a representation of the stria, such as a photograph, against a stored set. A number of best matches are then presented to the examiner for expert review.

But disparate IBIS have been set up by a variety of companies leading to problems in searching across records. To alleviate this, the US Bureau of Alcohol, Tobacco and Firearms operates the National Integrated Ballistic Information Network (NIBIN) Program. This has aggregated the various IBIS operated by government agencies to allow greater comparison of ballistic records [243]. Any agency wishing to join the NIBIN has to sign a Memorandum of Understanding with the ATF agreeing to maintain a base level of both equipment and expert staff to input records and assimilate results.

The field has been further advanced by the development of NIST’s Ballistics Toolmark Database [239]. This standardises the fields for meta-data about firearms images - such as calibre - but also introduces the use of an open source format for describing any stria [176].

The points to be taken from ballistics are that:

- like fingerprint examination, it is not a definitive topic - expert human judgement is required to decide if stria match;
- a classification system assists in this task by narrowing down the possibilities upon which an expert must opine - so assisting with the problem of selection; and
- centralised government efforts were required to form a common standard from the solutions put forward by the proprietary, competing, vendors.

2.4.3 DNA

For brevity, this section will not focus on how DNA was discovered but instead its use in criminal investigations - particularly relating to its initial challenges when used as evidence and also how classification systems have allowed international comparison to take place.

The first observation on the use of DNA for profiling was in 1985 [145] and its ability to differentiate humans for forensics purposes was recognised shortly after [113]. It was soon used as evidence of human identity in Court rooms - a practice pioneered in the US by private companies [13]. But by the late 1980s, its accuracy was sustaining successful challenges from defence lawyers. These attacks centred not on the theory and technology but the process by which the DNA extractions and analysis had been conducted.

It was argued that the private companies in their rush to have the DNA evidence admitted, and so gain market share, had “shielded their protocols and probes from rigorous scrutiny by claiming that they were proprietary” [13]. The FBI stepped in - providing standards and also training in how their standards could be attained.

But it was also recognised that standards were necessary for the recording of DNA - so that data banks could be built for comparison. Butler [45] describes the classification as Short Tandem Repeat (STR) Genotyping. This involves the calibration of the testing equipment being used before measuring peaks shown on fluorescent gel and converting them into a number. This number is then stored and compared with others. Final comparison is always conducted by the forensic scientist due to the need for fine interpretation of results.

The manner in which these "numbers" are collected and stored has varied between Europe and the US [220] but standardisation efforts have been driven by such bodies as Interpol, the European Network of Forensic Science Institutes and, in the US, the FBI. Whilst there are some variances, they are compatible.

The points to be taken from DNA are:

- whilst DNA has become a powerful tool for investigation, it was initially doubted because of private companies offering "black box" solutions without any specified standards; and
- standards for the classification of DNA results were not developed by the private sector but by government and governmental bodies.

2.4.4 What has been learned?

The construction and use of standards to describe findings is a strong element of all the reviewed disciplines. Also, these standards were not created organically but by a central body - often part of or related to a government. Finally, it is the marriage of automated systems applied to a classification system and human skill that has proved successful in these areas. The systems reduce the volume of results that the expert has to review.

When the topic later moves on to digital evidence, key issues will be:

- An assessment of whether digital evidence has the same classification systems that are present in the other areas reviewed?
- If it doesn't, is there a reason for this?
- Would the introduction of these classification systems help to address the identified challenges?

2.5 Factors influencing forensic examination

Aside from the lessons learned from current disciplines, there are other factors that influence the effectiveness of forensic evidence. These will be discussed because of their impact on digital evidence. First, the variety of evidence and then accuracy of interpretation will be discussed.

2.5.1 Variety is the spice of life

In describing forensic evidence earlier, three examples were deliberately chosen - due to their continued use. But what about other areas of forensic evidence - principally concerning the examination of trace evidence? Paint chips, gun shot residue, glass fragments, hairs and fibres, to name a few, have been valid and useful forensic science disciplines for many years but are now falling into disuse. The main culprit for this decline, Roux et al [213] argue, is DNA.

The development of DNA was so seismic that the resources it required pushed the others disciplines out of consideration. The traditional trace fields, though being described as having "robust and well established" scientific underpinnings, require costly laboratory equipment, well-trained staff and are time consuming. Further, they do not provide the personal identification or "individualisation" that DNA supplies.

In a number of papers Roux, Ribaux et al use Locard's exchange principle to argue that this is a retrograde step [205, 213]. The first consideration is Locard's intended meaning: whilst commonly cited as "every contact leaves a trace" they argue that this is a simplification of what was written and intended by the author. Instead they argue that the principle means:

- The types of material exchanged are dependent on the type of criminal activity
- These materials are the remnant of this activity
- Interpretation is required to transform these materials into clues of what activity occurred

They argue that trace evidence matters because, although it does not identify a person in the way that DNA or fingerprints can, it goes towards the holistic view of the crime - the building up of a picture showing what and how an activity could have occurred. This provides corroboration but also makes life harder for the criminal. They quote one of Locard's less well-known comments:

> *"Fingerprints are wonderful. I would say (.. .) it is privileged evidence. But, beyond, one can find prints of a variety of species: tooth print, nails, traces from the entire body, hair, dusts. Dust analysis is an infinite, unlimited resource. One can exactly know what the man did".*

The conclusion to be drawn is that variety of evidence is not something that should be shied away from - indeed it is positively beneficial. And when the problems surrounding digital evidence are examined, three things should be considered:

1. the approach to examining for potential evidence is to consider what traces are left when an activity takes place;

2. there should be caution on relying on any one particular trace or type of evidence. The mutual corroboration from a number of sources provides Roux's "holistic" view of events and helps to avoid misinterpretation; and

3. if multiple sources are checked, it is much harder for a criminal to adapt their behaviour to avoid leaving a trace. The more sources that are considered, the more they are constrained in their actions.

2.5.2 Accuracy of interpretation

Provenance is a commonly used term when discussing evidence - particularly forensic evidence. But the meaning of the word is somewhat ambiguous because it can cover at least two areas:

First, the origin of the actual data presented to the court. This could be a blood stain, a tyre pattern or a finger print from a murder weapon. This is the actual data and can be explained by showing a chain of evidence from an original item being first discovered with all the people who handled it explaining what they did and the processes that were applied.

But a second, key, use of the word covers the origin of the knowledge that is applied when this data is interpreted and presented as a forensic science finding. Why, for example, are the blood stains on the wall a blood spatter pattern? And why does it indicate that the victim was hit from the front? This is the area that will now be discussed.

The most recognised reference concerning these matters is the US case Daubert v Merril Dow Pharmaceuticals [247]. This gave guidelines on the admission of scientific or technical expert evidence.

Whilst these rules are often cited it is, perhaps, more accurate to consider the version captured later in 2000 by the US Federal Rules of Evidence [257]:

Excerpt from US Federal Rules of Evidence

1. the testimony is based upon sufficient facts or data,

2. the testimony is the product of reliable principles and methods, and

3. the witness has applied the principles and methods reliably to the facts of the case.

Welch [257], concerned about the admission of "Junk Science" into the Court room, notes that what is often called the Daubert "test" is not actually a test at all - it merely sets the questions and does not give any guidance for the correct answers.

Schwartz, in a dissection of the firearms and toolmarks fields' shortcomings [221] notes that the Daubert test has had little impact. Despite "systemic scientific problems" with these fields, as at 2005, no evidence of these types had been excluded. This is due to

the difficulty for non-experts, including judges, in assessing it - essentially marking the answers to Daubert's questions.

Schwartz's assertions on the firearms and toolmark fields may or may not be correct. But it does call into question the assertion that a method or tool must be correct and accurate because it has already been admitted at a Court hearing. It is not a particularly reliable indicator of efficacy.

The problem is not confined to the US. Robertson notes that in Australia "less than 5 percent of all matters examined in the laboratory will result in a forensic scientist giving evidence. An even smaller percentage of cases will see the forensic evidence being strongly contested" [207]. In essence, but for a small percentage of cases, the evidence is just accepted without test. This places an incredible burden on examiners to self-police the tools and methods that they use to ensure their reliability and accuracy.

Having looked at forensic evidence generally, the topic will now narrow to digital evidence specifically - what is it and how is it examined? But when the various digital evidence tools are later considered, one key aspect is the assertions made by the tools about the data they produce. On what basis are these assertions made? What precautions must a Digital Evidence examiner take?

2.6 Digital Evidence - the beauty and the beast

> *Some things can be predicted with reasonable certainty and this includes the continuing emergence of computer forensics as the new DNA for the forensic world. As every incident at any level of crime today has potential electronic evidence, it has been necessary to seriously rethink how best to use available resources.* Robertson [207]

This section introduces "Digital Evidence". First will be a discussion on what this term actually means followed by how the material is generated. The different fora in which Digital Evidence is used will then be reviewed before looking at current and developing challenges for the field.

Once these challenges have been articulated, the section moves on to look at approaches and tools that have advanced the field of Digital Evidence examination. The focus will be on how these respective approaches and tools can answer the research questions posed by this thesis.

2.6.1 What is Digital Evidence?

There are numerous definitions for the term "Digital Evidence". Carrier is general: "digital data that supports or refutes a hypothesis about digital events or the state of digital data." [52]. And so is Whitcombe: "information of probative value stored or transmitted in digital

form." [258]. Other sources reference that the field has moved on and should now be referenced as "Digital Investigation and Intelligence" [133].

But for the purposes of this discussion, Casey's narrow and applied definition will be used: "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi." [54, p. 7]. This concentrates on the evidential aspect and also how digital evidence is to be used in a criminal investigation leading to a criminal trial.

2.6.2 How is digital evidence used?

In considering how digital evidence is generated, a first view is that it primarily concerns computer or cyber crime

The Council of Europe's Convention on Cybercrime [73] broke down the field into four distinct areas which Walden [255], more succinctly rolls into just three:

Walden's Categorisation of "Cybercrime" [255]

Area	Description
computer-related crime	Traditional offences where the instrument for commission is a computer
content-related crime	The use of a computer to distribute illicit content - for example, copyright material such as films and music, pornography or more, recently, material to incite terrorism.
computer-integrity offences	The target of the offence is a computer - such as viruses or hacking.

But the increased use of technology as a general tool for life, especially the mobile phone, has led to a situation where evidence is generated out-with these arenas. As example, a man goes to a house and murders the occupant. He is carrying a mobile phone. The offence does not fall into the supplied cybercrime definitions: it is not used to commit a traditional crime or deliver illicit content and it is not compromised. Yet its location could be tracked using cell-site analysis - effectively placing that user at the scene of the crime.

So Digital Evidence can actually be generated as a "digital witness" to events. In the same way that trace evidence was shown in Section 2.5.1 to make a circumstantial connection between, for example, fibres on a suspect's jacket to fibres found at a crime scene, so digital evidence can link the user of a device to a location or an action.

And as its importance increases, following the commission of an offence, a role for investigators will be a form of digital "house to house" enquiries. But instead of asking the occupants if they saw or heard any of the events, the investigators will be checking to see if the occupants have any digital devices installed which will have inadvertently

collected digital artefacts. At present this may simply be the installation of a closed-circuit TV system (CCTV) but as the prevalence of technology increases, such as WiFi networks and the Internet of Things, more records will be generated.

2.7 Peripheral uses of Digital Evidence

Whilst the use of Digital Evidence in criminal investigations has already been introduced at section 2.1, there are other areas worthy of consideration. These include "Incident Response" and "E-Discovery". From the definition at Section 2.6.1 they may not always strictly make use of Digital Evidence - since they are not, necessarily, criminal investigations. But they are worth studying to understand the background to some of the tools that are later discussed.

2.7.1 Incident response

The terminology surrounding the investigation of computer emergencies - or Incident Response - has morphed over time. What Walden would call "computer-integrity offences" [255] - has become a more prominent topic in recent years and may be referenced using the term "cyber". But it is, by no means, a recent development.

In 1986, Clifford Stoll investigated the breach of computer systems he was administering [235].

In 1993 the concepts of "netwar" and "cyberwar" were coined by Arquilla and Ronfeldt [14]. *Netwar* relates to a high-level conflict where the target is a large group or population's opinion. It involves a multi-faceted attack involving interference with the media and tampering with networks and databases. *Cyberwar* is "traditional" warfare applied to information systems - both for enabling attack - such as smart weapons systems - and as targets - interfering with an enemy's information systems.

Since this earlier time, theory and practice have continued with public consciousness raised by incidents such as the unauthorised access to Sony Corporation's systems [22] and the allegations that Russia hacked the Democratic party's computer systems in the 2016 US elections [168].

The prevalence of these activities is documented but there should be caution if there is a mixing of investigators who are aiming to secure digital evidence with the intention of pursuing a criminal prosecution together with others looking solely at securing intelligence to prevent further attacks. There may be different thresholds on effectiveness of the tools and the degree to which they can be reliably interpreted.

2.7.2 E-Discovery

The term "E-discovery" has no strict legal definition but a relatively settled explanation would appear to be: a process by which "electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case." [156] echoed in [117].

The driver behind E-Discovery is civil and regulatory litigation - in particular the duty of a party in proceedings to make evidence available to another. When considering its application instead to criminal cases, aside from Lawton et al [156], sources [42, 82, 115, 146] focused on E-Discovery's ability to assist with criminal disclosure - logically mirroring its current use in the civil sector.

But the arena of disclosure, certainly in the UK, has a different focus for evidence than for investigation. The code covering this task [245], states the duty of the investigator is to review and reveal to the defence any material which may undermine the prosecution case or assist the version of events put forward by the defence. As such, the versions of events put forward by all parties are known. This provides targets for the material to review and, when dealing with selection, these targets can be used to reduce it. Most common is the use of keyword search - as later described in section 2.9.4

But at the beginning of a criminal case, the scenario and the parties involved are unknown - or only partially known. This means that the ability to focus reviews on any targets are limited until the enquiry is more mature.

The ability of E-Discovery's tools and techniques to provide a solution will be considered at section 2.9.7.

2.8 Current and developing challenges for Digital Evidence

This section looks at the challenges facing the use of Digital Evidence. It then examines what has been done to address them and, most importantly, whether these measures address the four fundamental problem statements posed by this thesis. These statements, originally defined at section 1.2, are repeated for easy reference. An examiner needs to:

- Understand the available artefacts on any particular data source (Availability);
- Be able to select which of these artefacts are relevant to a particular enquiry (Selection);
- Be able to to compare artefacts (Correlation); and
- Be able to document the provenance of an artefact - the reason why a particular piece of data indicates a particular event (Reliability).

The challenges being considered are the increasing volume and variety of evidence. As previously argued, these two issues are not the core problems facing digital evidence but, instead, factors that aggravate the situation when Availability, Selection, Correlation and Reliability are not addressed successfully.

Concern about the effects of volume and variety is not novel - having been periodically reviewed and visited by, for example, Carrier in 2003 [50], Hoss et al in 2009 [135], Raghavan in 2012 [201] and Lilis et al in 2016 [159].

In essence the arguments mirror those captured by the concept of "Big Data" - used as early as 1997 [164] and reiterated in 2015 [104].

Once the challenges posed by volume and variety have been defined, there will be a review of the tools and methods that have been developed to address these issues. The idea is to understand their approach and assess if they can answer the research questions.

The remaining gaps left by the tools will then be outlined. This will form the problem that is to be tackled in the rest of this thesis.

2.8.1 Volume of data

From early references to Big Data in 1997 [164] to the present day, the increasing volume of digital evidence has been a consistent theme. Quick and Choo, in their survey of papers published in the digital evidence field from 1999 to 2014 [200] reported over half of the ninety surveyed papers covered volume as a topic.

A recent report in March 2017 by the UK's policing inspectorate noted, despite special initiatives to clear digital evidence backlogs over the previous two years, there still remained over 16,000 items awaiting examination in the UK Police evidence stores [132, p.56]. The report noted understandable concern for this residue and that "sustainable" approaches were required to make best use of the opportunities presented by Digital Evidence.

Whilst the increase in volume is well documented, the reason why volume presents such a challenge is not so keenly articulated. Figure 2.3 lays out the effects.

First, volume is a phenomenon that is not all bad - greater amounts of data present more chances to find probative material. Further, it is much harder for a suspect to destroy it all.

But volume can have a negative effect on an investigation - both in the way it is processed and on the ability to locate evidence.

First, if there is too much material to review, valuable resources are tied up processing and reviewing it which could be otherwise employed. Further, as noted at Section 2.1, investigation is an iterative task - lines of enquiry change over time and, with consequently changing objectives, this means that increasing volume will adversely affect the investigation as a whole.

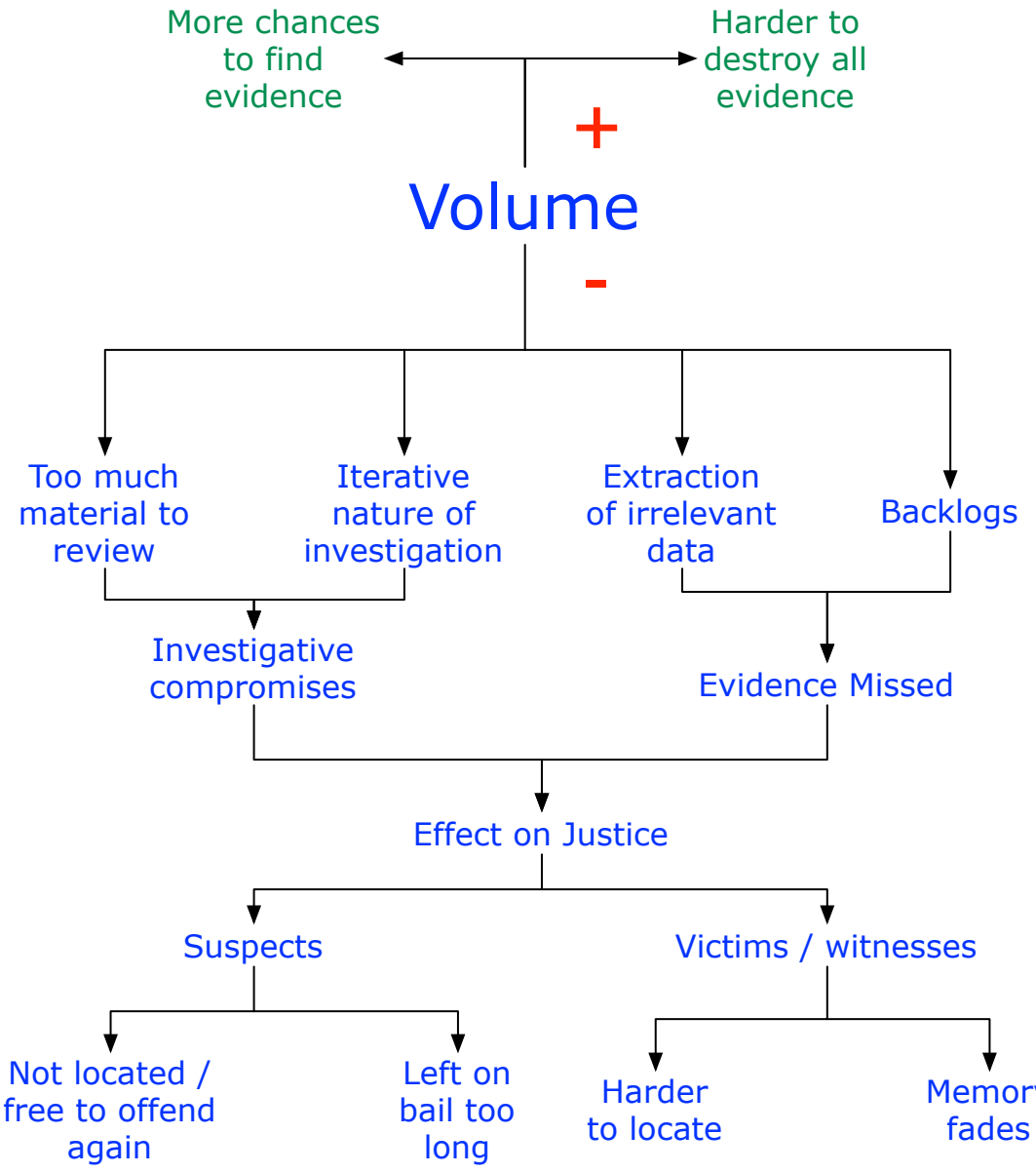

Fig. 2.3 The effect that increasing volume of Digital Evidence has on criminal investigations - both positive and negative

With existing resources but increasing volumes of data, each time the investigative objectives change logic dictates that the investigator must either:

1. review all of the data again and risk delay to the investigation;
2. selectively review devices that are considered most likely to contain useful artefacts; or
3. devise a method to reduce the volume of data requiring examination by distilling the evidentially useful artefacts from all devices for analysis.

Unless all material is reviewed each time, there is always a compromise to the investigation but practicality dictates that multiple complete reviews are not a viable approach. In reducing volume to facilitate review, there must always be a compromise and it is the way in which these compromises are made - and their effectiveness - that will be covered in section 2.9 on tools and approaches.

Together with the investigative compromises is also the chance to miss probative evidence: unless there is a carefully considered approach, merely trying to look at an increasing volume of material means that it is harder to discern that which might be of relevance from that which is not.

The investigative compromises and potentially missed evidence do have an effect on the Justice system. Suspects may not be identified and can destroy evidence, interfere with witnesses and commit further offences. On the other hand, suspects who have not been convicted may have to wait a long time for the results of the investigation and any trial. This is a considerable pressure - they may not be able to work and will suffer from the stressful effects of the situation. And they may be innocent.

But there is also an impact on victims and witnesses. As the investigation is delayed because of the Digital Evidence backlog, vital witnesses may not be identified and questioned. Memories may fade, records - particularly from mobile phones - may no longer be available.

So in mitigating the problem of volume, the challenge is to devise a method which makes the least investigative compromise and is sustainable.

2.8.2 Variety

Earlier, in section 2.6.2 the increasing number of sources for Digital Evidence was discussed. Casey [53] noted how the increasing use of digital devices for non-core computing purposes was producing the “digital dust” as described earlier by Locard. The use of processors in domestic appliance and home entertainment systems - as referenced by the term “Internet of Things” is producing data that could be most useful as a digital witness.

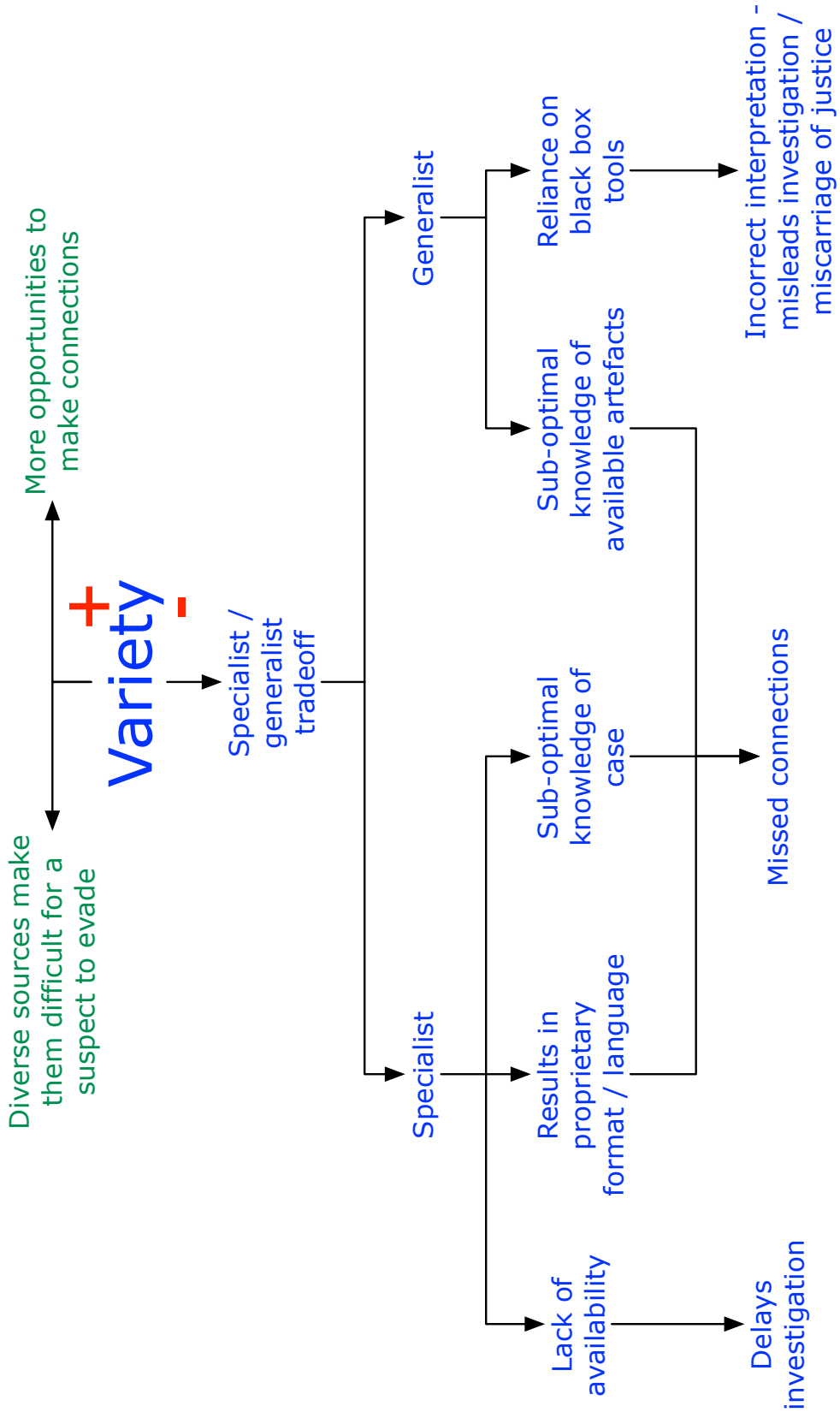

Fig. 2.4 The effect that the increasing variety of Digital Evidence has on criminal investigations - both positive and negative

For example, if a two person game was played on a Sony PS4 console followed by an increase in electrical power supply and the use of a washing machine on "hot" wash. This, in a murder investigation, could provide circumstantial evidence of two people present before an argument, the use of power tools to dismember the corpse and the washing of bloodied clothes afterwards.

This is not an abstract concept: in December 2016 news sources reported how investigators were making enquiries of Amazon's "Alexa" personal assistant in case it recorded words spoken during a suspected murder [256].

Casey notes the sheer pace of change in technology and how this is affecting digital evidence [56]: "the lion's share of digital evidence has migrated from wired computers to other systems, creating multifaceted challenges for digital investigators." This change produces different artefacts in increasingly disparate locations.

As with volume, the increase in variety, managed correctly, is a positive. The issues are shown at Figure 2.4. The diversity of sources means that suspects may not be able to keep track of all the digital records that are created as they commit a crime. For instance, a burglar may forget that his phone connects to a victim's home WiFi network. With correct identification and correlation, there are greater opportunities to make connections.

But there are drawbacks - chiefly centring on the diverse nature of these records. This can be categorised as the "Specialist / Generalist Trade-off" - a term used in the areas of evolutionary biology [152, 90] and personnel management [152] but not, specifically, in the field of digital evidence. The issue has, however, been debated in the general forensics field [213, 210] and, in some senses, mirrors the earlier debate on the gap between investigators and forensic scientists at section 2.3.

In summing up the debate, the specialist will have an in-depth knowledge of the field - knowing the artefacts that could be found. But, as noted by Harichandran [127], the way in which any results are described or presented may not be readily comparable with those from other specialist fields. Further, the specialist may not have case knowledge - raising a doubt over whether the most relevant artefacts will be identified and, if they are, will their significance to the investigation be noted. This can lead to missed evidential connections.

The generalist may be closer to the investigation but will not have such a detailed knowledge of the available artefacts - meaning some may be overlooked. Further, the lack of knowledge in a particular field may lead to the reliance on "black-box" tools as discussed at section 2.11.2. If the findings are not carefully interpreted then this can mislead an enquiry or, worse, lead to a miscarriage of justice.

Alink et al summarised the situation from a practical perspective: "it is difficult today to obtain an integrated view on the output of different tools. And again, it is quite unlikely that a forensic investigator has both the time and the knowledge to apply all appropriate tools to the evidence at hand" [5].

So, in dealing with the challenge of variety the problem is to devise a solution which:

- is able to keep track of artefacts on disparate sources;
- is able to select which ones are relevant to an investigation; and
- is able to correlate these artefacts no matter their original source.

2.9 Tools and approaches that have advanced the field

This section looks at solutions that have the potential to answer the research questions. This is from two perspectives: general approaches and tools.

General approaches are not necessarily designed for Digital Evidence but may still have the potential to assist. The tools are designed for Digital Evidence and are reviewed, first, from a theoretical perspective and then a practical one.

2.9.1 Testing and recording provenance

> *"Recently CRC Press published a book called Forensic Science — An Introduction to Scientific and Investigative Techniques... The reader is struck immediately by the scientific rigor applied to every one of the forensic sciences except digital forensics. Clearly, those of us using digital forensics need to be concerned about this problem."* Stephenson [230]

Earlier in section 2.5.2, there was a discussion on provenance - not just on the origin of a piece of evidence but what does this evidence represent? This will now be discussed in the context of digital evidence. This is important because of the fourth research question: reliability. A mechanism is required to document the provenance of an artefact - the reason why a particular piece of data indicates a particular event.

To aid discussion, provenance will be discussed as a number of levels - as shown at Table 2.1. There should be provision for each level for any item of digital evidence produced in a criminal trial. These levels can be used as a shorthand where some provision for testing and recording provenance is provided. If so, which level is it? And is there any provision for the levels that are outstanding?

If any software tool used by an examiner is "Closed-Source", more commonly known as "Blackbox", how do they satisfy the three levels? This will now be discussed.

When any forensic tool is used without the source code being available, this presents a problem since there is a limit to the amount of checks that can be conducted on its operation. The code cannot be inspected. To cater for this Wilsdon et al proposed a blackbox testing regime involving the generation of test cases and reference sets [260].

This idea was taken further by Buchanan [43] with the actual generation of these tests and data. The tests were simple - purely the recovery of files with no interpretation of their

Table 2.1

The Provenance Levels for Digital Evidence

Level	Question	How Answered
1	What data can be found in a certain location or structure and what is the justification for saying this?	Chain of evidence showing location of physical item and subsequent processes used to read / make a copy of data contained within any storage device. Efficacy of any software used to interpret at a higher level - such as parsing master boot records and file systems. Ability to repeat / reproduce by reference to definitive location - such as physical sector or file path
2	Has this data been successfully extracted and displayed correctly?	Justification that the data at a certain location can be represented as, for example, an IP address, MAC address or GPS coordinates
3	What can be inferred from this data? What does it "mean"?	Justification for asserting that the identified data item exemplifies an event or act - for example, the presence of a device in a physical location or the connection of the device to a particular network.

content. As such only a small subset of the functions were tested. Flandrin et al [101] in 2014 reviewed this and other previous efforts. They noted drawbacks in all previous propositions due either to the impracticality of the suggestion or that the proposal was too limited in scope to be effective.

The US government agency NIST has continued to test tools with its latest results published in 2015 [173]. The tools tested for computers are limited to:

- Wiping of media
- Imaging of media
- Hardware and software write blocking
- Deleted file recovery
- File carving

Whilst important, these are basic functions. Notable by their absence are tests on functions upon which examiners routinely rely:

- The interpretation of file systems
- The presentation of artefacts

It is of note that in its specification for testing mobile devices [174] NIST goes much further. The testing involves the successful extraction of user and device data in its tests MDT-CA-06 to 07 and MDT-AO-04 to 05[175] including the phone book, call logs, text messages, instant messages and third party application data.

This is only provision for level 1 and, possibly, level 2 provenance but not level 3. But these tests are an advance because of the breadth of coverage. However, the issue of variety has a direct impact on the usefulness of these tests:

1. Are the tests able to keep up with the rapid changes to mobile device hardware and operating systems?
2. In testing application data, how will the tests keep track of the variances caused by the interraction of different application versions, operating systems and devices?

It is understandable that NIST should seek to test only the core forensic software functions on general types of device hardware and software. It regards these a "head start on validating the tool" [173]. But the clear inference from this phrase is that NIST expects examiners to validate at least part of the tool's functions themselves.

Due to workload and, perhaps a lack of knowledge, Digital Evidence examiners have come to rely on computer forensic tools to, for example, interpret data from hard disk images or extract data from mobile phones. In using these comprehensive tools, sales literature has often made claims leading to an "industry myth that certain tools have been accepted by the courts" [166]. Whilst this comment was made in 2005, a review of these tools in Section 2.11.2 shows some are still doing so.

This is not a defensible stance for two reasons:

- first, as seen in section 2.5.2, just because evidence has been used in Court, it does not mean that it has been "tested". In fact, very little of it is subjected to informed challenge.
- second, the stance defies legal procedure in, at least, the US and the UK. Meyers records a commonly cited US legal judgement [166] deciding that software packages are not experts. Instead the material produced by the tool has to be presented by an expert after informed interpretation. Similarly, in the UK, there is no legal mechanism for the automatic acceptance of expert evidence from specialist forensic tools.

Even if the efficacy of closed source tools is accepted and they are properly operated, Stephenson's 2002 assertion [230] must be considered:

> *"Computer forensics comes fairly close, in process, to being rigorous, but, even here, the rigor is in the process, not the interpretation of data."*

To summarise the issue of testing and recording provenance, there are limited efforts to test the successful identification, extraction and presentation of artefacts. These efforts are limited due to the changing nature of technology - testing cannot keep pace. The testing that has been conducted provides assurance of Levels 1 and 2 Provenance.

But how is Level 3 provenance provided? Does, for example, an SMS text message in a mobile phone "Inbox" mean that the user received this message? And what do any associated dates and times mean - are they the time the message was sent, received or read? And if this level 3 provenance is not provided, what meaning will be assumed when this piece of data is used at a criminal trial?

2.9.2 Linked data

The concept of Linked Data was first discussed by Tim Berners-Lee in 2006 [28]. He cited what were to become known as the "Linked Data Principles"[31]:

- Use Uniform Resource Identifiers (URIs) as names for things;
- Use HTTP URIs so that people can look up those names;
- When someone looks up a URI, provide useful information, using the standards (RDF [40], SPARQL [242]); and
- Include links to other URIs, so that they can discover more things.

The purpose of these principals is to provide a foundation enabling the linking of disparate data sources using the Internet. This resonates with the third research problem: correlation - providing a classification scheme to compare artefacts.

Some applications of Linked Data have been found in the Digital Evidence field:

- Dosis [84] uses Linked Data principals to join events to times whilst Gayed et al [110] propose their use for proving evidential chain of custody;
- Syed et al [236] propose a "Unified Cyber Ontology"(UCO) which, in its prototype form, models software vulnerabilities. The benefit of using Linked Data principals is that the model can link to other external data sets to perform compound queries; and
- Nimbalkar et al [179] build on the UCO work to show how log files can be broken down into their component parts and links formed between them.

But whilst the concept of Linked Data shows promise, the development of the field for digital evidence is still in its infancy.

2.9.3 Triage

Triage is "the process of determining the most important people or things from amongst a large number that require attention" [189]. Whilst it is used in the digital evidence field there are differing approaches to triage with the process described by Shaw and Brown as "poorly defined and poorly understood" [223].

One approach is to have an early, targeted, inspection of the evidence for any material of apparent assistance [209]. This is a tactic employed by the UK's Metropolitan Police to look at mobile phone data [132].

The second approach is described by Parsonage as "a process for sorting enquiries into groups based on the need for, or likely benefit from, examination" [193] and echoed by Clarke [67].

Quick and Choo [200] propose a third approach where a subset of potentially relevant files is extracted and analysed in place of a full image.

Concerns about triage have been expressed [144, 198, 212]. If triage is used by non-experts in advance of a full inspection, are they able to accurately interpret any results. If used by either experts or non-experts, to select devices for a full examination, what criteria are used?

In summary, there may well be a case for the use of triage but its effectiveness depends on the tools looking for the relevant data in the correct location. The surveyed papers gave no indication of how this was to be achieved.

2.9.4 Keyword Searching

Whilst the concept of keyword searching is a basic one with little need for explanation, it is still a fundamental tool to sift through data. The function has moved on to conceptual or fuzzy matching of words [156] but these are variations on a theme.

Despite being one of the most commonly used forensic techniques, it is only of use when the likely keywords are known. This is problematic at the start of a large complex conspiracy investigation as those words may not be readily apparent.

For example, in the insider dealing investigation of Matthew Uberoi et al [155], the son was working in an investment bank and sent his father coded instructions to buy shares in the guise of an order for takeaway chinese food. At the early stages of an investigation, these details were not known. Only after examining emails and noting that the messages were suspicious - no one could eat that much chinese food - was the connection made and the keyword search for "chinese" run.

This shows the limitations that can be encountered when using keywords for, example, the triage of devices. The significance of the word "chinese" would not have been known at the start of the case and its presence on any device would not have been important.

Keyword searching does not assist in assessing availability and selection since it is run across all data - unless some culling has first been conducted using some other method.

Similarly it does not assist with correlation since, without some form of classification system, it is assessing whether any piece of data on a source matches the keyword and, again, this depends on first knowing the correct keyword.

2.9.5 Time-lining

Time-lining is, effectively, getting a number of events or pieces of data and lining them up in time order. It is cited as a valuable tool for digital evidence examination [60]. Indeed in the Operation Saturn insider dealing trial [99], the time-line of evidence from disparate sources provided compelling evidence of suspects looking at confidential documents before transmitting them to accomplices.

But there are three problems with the approach.

- First, the volume of time stamps in modern digital devices can be a challenge. As noted by Gudjonsson [122]: "A super time-line often contains too many events for the investigator to fully analyze, making data reduction or an easier method of examining the time-line essential." But if the examiner is selecting only particular records to put in the time-line, how is this selection made?

- Second, there may be variances in the time stamps due to inaccurate clocks, time zones and the very manner by which they were created. As Schatz notes: "all but the simplest of forensic investigations will involve multiple computer time sources in various states of de-synchronisation" [217]. If the clocks are not aligned, or if the times they represent not unified, then a time-line is not only of little use but also hazardous as evidence will be missed. This affects any ability to answer both the correlation and reliance questions. Methods have been proposed to check for accuracy by, for example Willassen [259] and Schatz [219], but these will only be effective if they keep pace with the increasing variety of data sources.

- Third, time-lines are only useful in certain scenarios - normally at an advanced stage of the investigation when the facts are well established and there is a desire to impose some order on them. Even some tool developers warn on this aspect: "By limiting a search's scope to only a particular date or time, or even a range of dates or times, investigators may miss important and relevant information: an argument that occurred several weeks before the homicide, for instance, or a pattern of harassing behavior with more victims than just a single complainant" [59].

When considering the limitations outlined above, time-lines do not assist with availability or selection - some other method must be used. But time-lines do assist with correlation as long as some method is found to first unify both the times and their semantic representation before inclusion.

2.9.6 Hash functions

The use of Hash functions such as MD5 [206] and SHA-1 [78] feature prominently in many aspects of digital evidence. They are a way of generating a code for any piece of data that is unlikely to be generated for any other different piece of data. Since files are just a "piece" of data, this means that they provide the ability to recognise files - and the differences - based on whether or not they generate a particular hash code value. Identical files will generate the same value.

It is not the properties and operation of hash functions that are pertinent for this discussion but, instead, their ability to address the four research questions.

In essence, hash functions can be used to filter out extraneous material or look for potentially relevant material.

For example, NIST maintains the National Software Reference Library (NSRL) [172] containing the hash values of files from common operating systems and applications. This means that the files on a device can be hashed and compared against the NSRL library to filter out files which are unlikely to contain relevant material. Alternatively, they can be used to look for the presence of particular applications.

Garfinkel et al [105] use hash functions to search across large volumes of data . The targets are known files and their fragments or, instead, fragments of known data structures such as those found in JPEG files. Statistical sampling methods are used to reduce the volume of data that must be checked. Roussev [211] shows how "data fingerprinting" can take the characteristics of a file for comparison rather than having to search for all of it.

Whilst a valid technique, hash functions do not address the research questions. They do not assist with knowledge of available artefacts or their selection. They do not ensure that data values are in a consistent format to aid correlation. They do not provide any assistance with reliability.

2.9.7 E-Discovery

Earlier, at section 2.7.2, E-Discovery was introduced. As a reminder, this is a process by which "electronic data is sought, located, secured, and searched with the intent of using it as evidence in a legal case" [156].

The process is largely concerned with civil and regulatory cases though is now making in roads for disclosure exercises and the investigation itself [156]. For this reason it has been reviewed.

A common reference point for E-Discovery is the Electronic Discovery Reference Model (EDRM) [86] which is illustrated at Figure 2.5.

A review of this model shows the "Identification" phase could assist with the selection problem because it aims to locate and understand potential sources of electronically stored information. But the EDRM offers guidelines which, though informative, are high level check lists of the activities to perform. And no material based on the EDRM was found

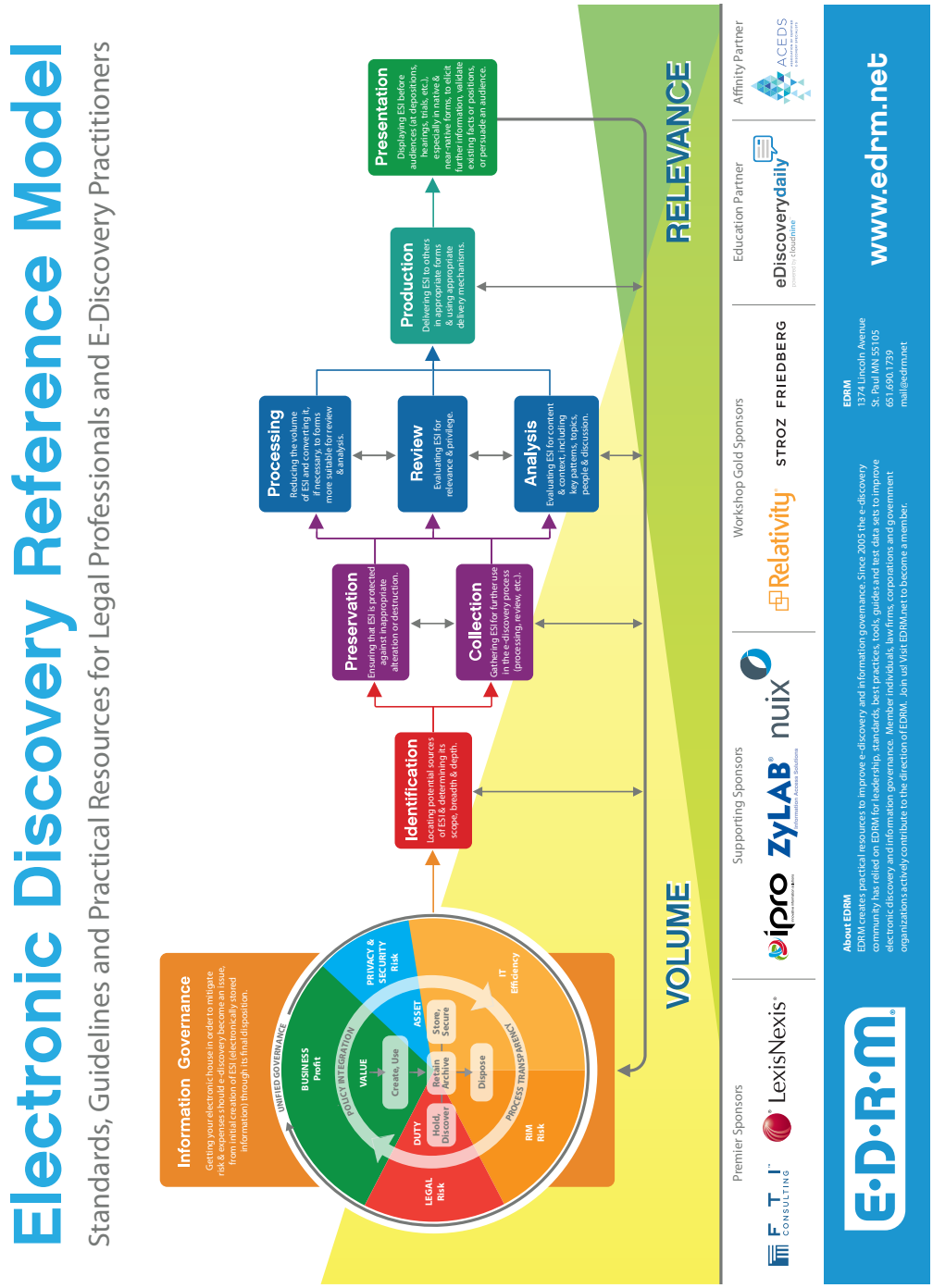

Fig. 2.5 The E-Discovery Reference Model (EDRM) [87]

that would further assist in identifying what digital material was available and how any selection could be performed.

The EDRM's Processing, Review and Analysis phases aim to:

- reduce the volume of data and convert it into a reviewable form;
- evaluate it for relevance; and
- evaluate it for content - such as topics and people.

If successful, this would address the questions of selection and correlation. But, essentially, the tools being used to perform these functions are keyword searching and categorisation by file type and time - a form of time-lining. The benefits and disadvantages of these have already been covered.

Further, as noted by Lawton [156], E-Discovery is centred on user generated material such as documents, spreadsheets and emails. This is not the breadth of data available on devices. Finally, a key driver for digital investigations is to locate evidence but for E-Discovery it is about managing costs.

Lawton's review - the only paper found examining E-Discovery tools from a criminal investigation perspective - noted that there were advantages to the contemporary tools:

- the ability to convert data from disparate sources into a common format such as XML; and
- the presentation of a common interface for this data.

This could assist with correlation. But it did, however, note that the commercial tools were "generally poor at helping the investigator to understand the links between their data and spot new investigative leads". An example of this is its XML coding [88]. This contains a limited number of classifiers which all relate to either email header fields or file meta-data such as size and creation date.

2.9.8 Digital Evidence artefact / information repositories

This section looks at attempts to record information about Digital Evidence artefacts. If effective, any repository could answer the availability question and may assist in selection and correlation. They will reviewed with these possibilities in mind.

The Forensic Wiki

The Forensic Wiki was first established in 2005 [238] and covers "information about digital forensics". This is not limited to artefacts but also covers "tools and techniques used by investigators".

The Wiki shows a healthy usage - currently consisting 856 pages with regular additions. There is no data to understand how commonly these pages are referenced.

The pages are organised in a tree-based category system - 13 main categories, discounting three for administration, and further sub-categories. The "Tool" category, for example, has a further 12 sub-categories covering such topics as "Disk imaging" and "Vaporware".

Aside from these categories, there is no structured tagging system and so searching the Wiki for topics pertinent to a particular digital evidence source would not be possible.

The Artifact Genome Project

The Artifact Genome Project (AGP) [15] is an an "online system for uploading and viewing digital forensic artifacts". Its initial development came from documenting "cyber observables" as described by the CybOX project [77]. This concentrates on system-wide attacks in the Incident Response field as documented in section 2.7.1.

In terms of classification, before submission of an artefact to the AGP, a user must first select an artefact type - which includes File, Windows Registry, SMS Message and Email. A unique name must be chosen and the type of entity that created this artefact must be chosen - for example: User, System or Network.

In specifying the Device upon which this artefact was found, the description is not broken down into its constituent parts - such as device, file system and operating system. It is instead listed complete, for example "Computer, Windows 10, 64 bit, NTFS".

Other data items are captured - such as date and time of the artefact's discovery and subsequent addition to AGP and the person discovering it.

AGP invites users to also submit the reference sources used for any submission.

To search AGP, the artefact type, device type and other entered criteria can be selected together with the use of keywords.

Observations on AGP are as follows:

- The project has momentum - at the time of review it contained 439 artefacts and it is being actively publicised to garner more entries [264];
- It is not clear if AGP stores information about artefacts or the actual artefact data itself. For example, its SMS Message Artifact template invites completion of the Sender and Recipients' phone numbers but its "Email Windows 10 AOL Content" artefact documents the folder where AOL email messages are stored.
- In addressing availability and selection, AGP's artefact classification system limits the assistance it can provide:
  - Because devices are listed in a system format - ie combining the device type, file system and operating system together - there may be a lack of flexibility. For example, the NTFS file system has artefacts contained within it that are irrespective of the operating system. There is no mechanism for recording these artefacts.

  - There is the potential for ambiguity in the terms employed by AGP and this is shown when conducting searches. For example, the network Media Access Control (MAC) address is a common and useful identifier. But, in AGP how does a user search for any artefacts that relate to the MAC? A search for 'MAC' on its keyword and Tags function both returned hits relating to "Macintosh". And further, even if there was a specific tag for "MAC" would this relate to the Media Access Control or a Message Authentication Code?

- Some of the listed artefacts do not provide sufficient detail to provide great assistance to an examiner or be readily searched. For example the "File iOS 10.3.1 Wifi Connections" artefact states it contains data relating to WiFi connections. But it does not document the positions in the referenced file that these discrete data items can be found. Further, it does not explicitly list the - earlier referenced - MAC addresses that can be found in this file.

The observations indicate that the AGP could be a valuable addition to the field but to assist with the four research questions there needs to be clarity on the data that it is trying to represent. It also needs a controlled vocabulary with structure so that users are able to better understand the artefacts it contains and how it can be searched.

Magnet Forensics Artifact Exchange

In 2017, Magnet Forensics created the Artifact Exchange [161]. This is not an open-source repository and it has not been possible to review it.

2.9.9 Repositories: summary of findings

The Forensic Wiki and AGP both aim to increase awareness in the digital evidence field.

Both of these repositories suffer from a lack of controlled vocabulary. Without this, names and terms will lack clarity and there is a danger of capturing irrelevant information as well as the pertinent artefacts. This makes them difficult to search for the available artefacts on a particular device and there is no method for selection based on investigative need.

2.10 Previous research on digital evidence tools

Before considering the tools that have been developed to examine digital evidence, it is worthwhile examining the research has been conducted into these tools. Are the Research Questions addressed by the tools - or do the tools seek to answer different questions?

The review stems from some of the earliest studies in 2003 to the present day.

2.10.1 Comments on provenance

There is significant comment on provenance. Carrier [50] in 2003, and to a greater extent, Wilsdon et al in 2006 [260], argued that tools, whilst providing access to evidence do not allow verification of the evidence's reliability - essential if digital forensics is to approached from a "scientific point of view". To improve the situation, abstraction layers were proposed - this breaks a tool down into the functions it performs with the output from one function feeding into the next. Each layer can be independently tested to understand if it performs its intended function accurately and completely.

Beckett et al [23], in 2007, noted how examiners relied on vendors to validate the tools they produce yet this validation is often undocumented and unproven. Whilst one method of testing could be the use of two different tools to understand if they achieve the same result, this takes no heed of the possibility that both tools could be wrong.

Instead it was argued that the development of individual forensic tool testing can be avoided if a neutral stance is adopted. A predetermined function is contemplated with the tool tested against its ability to perform this function using a defined reference set. This carries on the earlier proposal of layers.

This means that, first, the choice of a tool is irrelevant so long as it can demonstrably perform this function. Second, testing new iterations of a particular tool is simplified - simply run its functionality against a reference set and verify the expected results. Guo et al [125] in 2009 and Casey [55] in 2012 echo this view.

On the surface, this proposal may not seem particularly novel but, in fact, it is because of the shift of focus from the tool to the function. As new forensic artefacts are discovered, the consideration is selection of a tool that can accurately perform the required function - ie extract this artefact. As Becket [23] notes, this is a new paradigm.

The 2015 publication of the NIST tool testing handbook [173] saw a comprehensive review of a large number of digital forensic tools. In a sense, it begins the journey outlined above because it conducted tests on only certain capabilities of a tool. They are intended only as a baseline on top of which examiners can subsequently conduct their own tests. The difference is that, instead of breaking down the tool into functional layers to test, it tests certain functions of a whole tool.

2.10.2 Comments on availability, selection and correlation

Ayers [17], in 2009, argued that "tools are not keeping pace with increased complexity and data volumes of modern investigations." These "First Generation" tools concentrate on the extraction of files but Ayers argues that the examiner's purpose is not to locate relevant files but, instead, relevant evidence.

The necessary attributes of second generation tools that address these problems are defined by Ayers. These attributes are predictable: fast processing speed; accuracy and

reliability; auditability and repeatability; and data abstraction. There are possibilities outlined for how these attributes may be gained without any concrete proposals

The same year, this view was echoed by Beebe et al [24] noting that the goal of tools should be to provide "information and knowledge, not merely data". This includes "automated link analysis" and "cross-correlation". It asks why digital forensic tools did not yet meet the needs of examiners?

In a prescient review in 2010, Garfinkel [107] argued that the tools developed in preceding years would be unable to cope with future challenges including:

- increasing volume
- increasing variety creating difficulty in extracting artefacts and then correlating them across sources
- the change in media storage devices - such as mobile phones - making live acquisition a necessity
- encryption
- cloud-based storage

In a practical suggestion to address these problems Garfinkel argued that there is a requirement for the creation of a "a wide range of abstractions - standardized ways for thinking about, representing, and computing with information ranging from a few bytes to a person's lifetime data production."

Raghavan's 2013 survey [203] included an examination of a forensic tool's ability to "compose" evidence using meta-data from heterogeneous sources and identify correlations. In some part, this was testing whether Garfinkel's earlier suggestion had been implemented. The eleven surveyed tools included four of the, then popular, commercial offerings. Only one was found to provide such correlation and this was based on keywords.

Raghavan noted that the tools relied on the examiner supplying the appropriate keyword or attribute for comparison but, of course, should the examiner not supply the correct criteria, the pattern would be missed. Further, few of the available meta-data - aside from IP addresses, user names and timestamps - were considered. This leaves a large amount of them under-utilised.

In 2013 Salem et al [216] noted the increasing diversity of mobile devices and the inherent difficulty in selecting the correct tool to perform an examination. They warned how selection of an incorrect tool could lead to "compromised evidence, incorrect interpretations and wrong conclusions".

In 2015 Katie et al [149], in their taxonomy of digital forensic challenges, noted increasing volume and also how forensic tools designed to cope with the various devices are incompatible with each other. In essence, there is no system allowing the outputs from these tools to be correlated.

2.10.3 Summary

Over a long period of time, the research questions of availability, selection, correlation and reliability have been continually cited by researchers. Yet contemporary reviews of tools do not identify efforts to address these questions.

The following section looks at these tools to verify this point and, if proven, why this is the case and how it could be addressed.

2.11 Digital evidence tools

This section reviews tools from two perspectives: modular and monolithic.

Modular tools are those which provide a framework to intentionally allow the incorporation of various other "plug-in" tools to perform a certain task. Of those surveyed, they are largely open-source and require a greater level of technical knowledge to operate than monolithic tools.

Monolithic tools are more restricted in their ability to integrate with other tools but offer a more user-friendly interface. They are designed to offer a platform where all required tasks can be performed on a particular source. Of those surveyed, they tended to be commercial.

The review of monolithic tools is based solely on the information from the various companies' websites and material they make available such as "white papers". On the face of it, this is not comprehensive - a fair evaluation would involve trialling the products.

However, the point of this exercise is to understand how an examiner would select a tool to use? If there is a limited budget to purchase a Digital Evidence examination tool and limited time to learn its operation, how does an examiner decide which one will fulfil the investigative objectives?

2.11.1 Modular Tools

Hansken

The Netherlands Forensic Institute first released a product called Xiraf [5] which was further developed to produce Hansken [251]. The documentation describes more of an approach than a tool. Further, although knowledge has been built up through considerable practical application, the tool appears to be commercial: no open source download or trial evaluation was found. As such, only a limited assessment can be conducted.

Essentially, Hansken states it uses a modular approach to process data from any source so that it can be viewed through one web interface. Analysis can be conducted by keyword search, time-line or selective review of evidence types - such as chat messages.

Whilst there are information security controls built into Hansken, it does appear similar to an e-discovery system. There is insufficient documentation to understand if it goes

further than the user created data such as documents, spreadsheets and emails that these systems would handle.

Documentation states that it can handle data from many sources but there is no detail.

The sparse documentation means that it is not possible to assess its approach to the Research Questions.

Google Rapid Response

Google Rapid Response (GRR) is principally an incident response framework - a tool for collecting data from live systems suspected of being compromised or involved in compromise [69].

It aims to provide a centralised source of artefacts that is free and compiled by the general community. Castle, [58], reasons that during incident response, there is a need to retrieve common pieces of information whose location and format may vary across heterogeneous systems. These need to be collected and grouped automatically - without respect to the source - ie they should be comparable.

This approach has benefits:

- first, this assists with availability as there is a list of artefacts to reference; and
- second, the ability to compare artefacts across a variety of sources addresses the question of correlation.

However, when examining the store of GRR artefacts it is clear that there is some work to be conducted before the goals are realised. The location of artefacts is not stated in sufficiently granular detail to allow easy and effective extraction. For example a location of Microsoft Office Most Recently Used (MRU) on Darwin (OS X) systems is listed as:

- %%users.homedir%%/Library/Preferences/com.microsoft.office.plist

But this is only the location of the file that contains this data - not the location of the data within that file. This further detail can only be implied from reviewing the python code specified in the supplied reference. As such, this is not platform agnostic or automatically parsable. An improvement would be to have the explicit location of the actual data item specified in the artefact entry.

GRR also has a stated aim of grouping artefacts and its style guide [165] sets out definitions for these groups using “labels”. Examples are:

- Browser: Web Browser artifacts.
- Memory: Artefacts retrieved from memory.
- Rekall: Artefacts using the Rekall memory forensics framework

These may be sufficient for incident response but offer little utility for criminal investigations:

- first, they are too broad to allow proper comparison across heterogeneous sources with no specification for reporting format; and
- second, they are drafted from a technical perspective which does not allow an investigator to understand which artefacts could assist in a line of enquiry.

Bulk Extractor

Bulk Extractor [108] searches for patterns across any digital source. These patterns can be in the simple form of, for example, IP addresses, email addresses or telephone numbers or the more complex, such as patterns that identify a particular file type. This now extends to "SQLite" databases [33] - currently a common storage point for mobile phone applications.

The idea behind Bulk Extractor is that it is source neutral - acting on any digital stream - and is blind to the file system - looking only for patterns. Because of this, the approach to availability and selection is not device specific. Instead, availability relates to those patterns for which Bulk Extractor can search and selection relates to those patterns that are chosen.

In terms of correlation, Bulk Extractor's radical approach has both positives and negatives. First, its media and file system insensitive approach means that an examiner can handle data from any source. Further, its ability to search for a pattern and output this in a consistent manner aids easy correlation - as noted by Garfinkel [106].

But this very approach of media blindness also has an impact: first, more data may be processed than is necessary when compared to GRR's approach of identifying a particular artefact in a location and just extracting that data. Second, as noted by Bradley et al [33], the scanners are limited when discussing false positives. Care is required when interpreting them. The reason for this caution is that the position of an artefact within a file and the location of that file within an operating system are key to any interpretation. Bulk Extractor, on its own, does not provide this information.

Sleuthkit and Autopsy

"The Sleuthkit" and its front-end, "Autopsy" [240] are an open source framework for processing any digital media.

Essentially, the file system is processed and the material made available for keyword search, time lining or selective review of contents. Third-party modules are available to, for example, ingest Windows Pre-fetch files [226].

There is a facility called "Interesting files" which aims to bring any predefined objects of note to the immediate attention of the examiner. This was also noted with Bulk Extractor using "watch lists".

In terms of availability and selection, no assistance is provided by Sleuthkit. In terms of correlation, although Sleuthkit is adapting to various disparate media - it now parses material from Android operating system devices - it does not use any form of uniform data representation or categorisation. Further, its third-party module developer instructions [226] has no specification in this regard.

If Sleuthkit could be married with a central source of artefacts then its effectiveness could be improved.

2.11.2 Monolithic Tools

As earlier referenced, the term "monolithic tools" is used to describe comprehensive tools that are designed to provide an all-in-one solution to processing and examining digital evidence.

There are benefits to this approach: a consistent interface allows easier control of the tool; and, properly implemented, the tool should be able to correlate disparate artefacts across the sources on which it is used.

In the earlier review of research on digital evidence tools in section 2.10, criticism was levelled at these tools but no definitive analysis of the digital evidence tool market place has been identified. Certainly, whilst there may be some justification to the criticism, there also needs to be consideration of the role that the developers are trying to perform. They are driven by the demands of their clients to handle increasing volume and variety - already discussed at sections 2.8.1 and 2.8.2. This leads the tools to focus on these issues. But this thesis argues that volume and variety are aggravating factors for digital evidence examination - not the underlying problems.

A number of tools will be briefly reviewed. Comments in this review are not intended to downplay the significance and utility of these tools but to document how the tools could answer the research questions in whole or part.

For brevity, it should be assumed that all of these tools provide facilities for keyword and pattern searching, time lining and selective review of extracted contents. A deeper look at certain specific tools takes place at section 6.5.1.

The available literature of the following tools was reviewed:

- ADF Triage [2, 3];
- Encase Forensic [124, 92];
- Forensic Toolkit (FTK) [1]; and
- Nuix [181, 182].

Availability of artefacts

Of the documentation reviewed for these tools, there was no material which described the artefacts that are available for a particular device and, of these, which ones could be extracted by the respective tool.

As examples, Encase's promotional literature states that it supports the "widest array of computers, smartphones, and tablets of any forensics software solution" but there is no listing of these devices or respective artefacts. And FTK states that it handles operating systems such as iOS and databases such as SQLite but does not state what artefacts it extracts from them.

Selection of artefacts

All the tools allowed selection based on keyword search and file system meta-data such as creation date.

Where the surveyed tools allowed more sophisticated selection of artefacts, this was on a technical process. For example ADF has categories such as "APPLICATIONS > Application Usage".

Nuix differs slightly in that it states that it can automatically retrieve and correlate: "company names, sums of money, email addresses, IP addresses, and social security, phone, and credit card numbers". But it is not clear if this is also conducted on keyword and pattern matching or if some internal categorisation is used. As such it was not possible to assess.

Correlation of artefacts

The only one of the surveyed tools to explicitly discuss correlation was Nuix. As detailed above, its selection process specifically details the extraction of such values as phone and credit card numbers. The success of correlation will depend on whether some sort of classification system is employed to ensure that, for example, the same phone number, stored in different formats, is matched.

Also of note is that Nuix, certainly in 2014, was actively promoting the ability of its product to operate with other tools. It has published an Application Program Interface (API) but, again, there is no data classification or formats listed so this limits any assessment of correlation.

Reliability of artefacts

Terms such as, "Forensically Sound", "Court-cited" and "Court-acceptance" were used in the surveyed literature. The possible hazards of using these terms has already been explored at section 2.5.2.

Level 1 provenance was documented - where the artefact value was found - but there was no mention of Levels 2 and 3.

Summary of monolithic tools

The surveyed tools suffer from a lack of technical documentation. This presents difficulties when reviewing their effectiveness in addressing the research questions.

There is no documentation of the artefacts that are and are not covered by a tool - so how is an examiner able to assess their completeness? Selection of these artefacts is either from a technical perspective or from a category named, for example, “Application” usage . There is insufficient description for an examiner to assess what this category covers. There is no documented facility to effectively correlate artefacts from different sources and no documentation on the justification for a particular artefact.

How could monolithic tools be improved?

There are two improvements that would enhance the use of these monolithic tools.

First, if there was a uniform listing of artefacts, a tool could explicitly state which of these it is able to extract. Essentially, this takes the onus of identifying this data away from the developers and leaves them to produce fast extraction tools.

A further benefit is that these artefacts could then be organised from an investigative perspective rather than a technical one.

Second, if artefacts could be extracted from these tools with a uniform type and format, then this data could be readily compared with other tools and shared amongst investigators. In a manner, this is an extension of the formats specified by the E-Discovery Reference Model.

This second point appears to be gaining some traction with the recent announcement of the Cyber-investigation Analysis Standard Expression (CASE) [20, 94]. Developers, including all of the surveyed monolithic tools, have expressed interest in this project and it could provide a core foundation for the expression of artefacts and their comparison across sources and tools.

The project aims to address the shortcomings identified to date. In particular: allowing the communication of artefacts in a standardised form; maintaining provenance; and providing support for structured and linked data.

In terms of addressing the research questions, it does not assist in assessing the availability and selection of artefacts. It is not a library of what may be available, it is a method for documenting what has been found.

In terms of correlation, the design is still at an early stage but inspection shows it to be principally concerned with documenting the technical details observed on a device - such as “BrowserCookie”. It has already published mappings of how, in one example, the results from a mobile phone examination tool can be mapped to a central set of terms [241]. This aids correlation because the results of other tools, which are also mapped to this central set of terms, can be compared.

Where it has not yet been developed is to document which items of data within a "BrowserCookie" would be of use to an examiner and providing a uniform format for them to be reported.

In terms of reliability, it addresses Level One by documenting not just the source of the artefact data but also the tool that was used to extract it. But not Levels Two or Three which form part of what is referenced as "Evidence Analysis".

2.12 Conclusions

The first research requirement, detailed at Section 1.1, called for a thorough examination of the issues that need to be addressed to see an improvement in examination. These are availability, selection, correlation and reliability.

The review of current non-digital evidence sources at section 2.4.4 found that the use of classification systems to document findings has been a key factor in their success. This has allowed selection and correlation of artefacts.

The review of both theory and practice of digital evidence tools at section 2.10 found that no such a classification system has been developed so far.

The development of CASE, detailed at section 2.11.2, shows promise in documenting the results of tools. But first, it does not assist an examiner to know what artefacts may be available and which ones to select. And, second, its current manifestation is at technical level and there is still a challenge in mapping these results to the investigative questions that require answers.

Whilst some systems aim to document the location that data was found together with the method and tools used to extract it, there is still a gap in establishing Level Two and Three provenance - why a piece of data can be represented in a certain way and what does its presence mean?

But the benefits of a suitable classification system that were seen in the three previously reviewed forensic evidence fields could also alleviate the problems seen in digital evidence for the following reasons:

1. artefacts could be compared, irrespective of source or the tool used to extract them;
2. artefacts could be selected based on the particular investigative questions that require answers;
3. the burden of provenance would be alleviated if tools merely had to be proven to extract a particular artefact rather than also attempting to interpret it; and
4. a tool could list which artefacts it covered - so allowing the examiner to select the most appropriate one.

The research questions posed by this thesis are documented at section 1.2 but are repeated for convenience:

Principal Question

- **RQ1:** Can a classification system be devised that allows for the documentation of digital evidence artefacts and facilitates their extraction and comparison?

Availability

- **RQ2:** How can this classification system allow for differing digital sources and rapid changes in technology?

Selection

- **RQ3:** Is it possible for this classification system to reduce the volume of digital evidence that requires examination?
- **RQ4:** Can this classification system allow for the selection of artefacts based on investigative criteria as opposed to technical ones?

Correlation

- **RQ5:** Can the classification system allow for successful comparison of artefacts irrespective of their source or originating format?
- **RQ6:** Can the classification system allow the use of any tools to process evidence?

Reliance

- **RQ7:** Can the classification system provide for the provenance of these artefacts to be established?

The use of a form of model called an ontology is proposed for this classification system.

The next chapter continues the first research requirement's thorough examination of the issues. First it explains models and ontologies and then goes on to review the field to understand how existing ontologies could help to answer the research questions and where there are gaps.

Chapter 3

Related Work

3.1 Introduction

The previous chapter provided background on investigation and its use of forensic evidence. The focus then moved to the examination of digital evidence and the challenges it faces. After examining approaches and tools used for this field, gaps were identified when considering the research problems.

It was proposed that a classification system could answer these questions. This leads on to the Hypothesis detailed at Section 1.1 - that an ontology can improve the effective examination of digital evidence in large criminal cases.

This chapter introduces ontologies and allied models. In so doing it justifies the choice of this format for classification.

First, the terminology will be examined. Included in this discussion of models and ontologies will be an allied topic: digital evidence taxonomies. The reason for this discussion of terms is to highlight their evident ambiguity. For this reason, when previous research is then considered, it does not strictly stick to ontologies. The reason for this consideration is that it is not just whether any of the previously specified ontologies are suitable for re-use but if any of the models or taxonomies have ontological properties which make them also suitable for such re-use?

The review of the various models that have been developed is then detailed. The analysis takes in quite a lengthy period of time because, as will be seen, some of the fundamental challenges of digital evidence were recognised from quite an early stage and it is useful to understand the solutions that were proposed and why they were not successful?

Following this, ontologies will be covered - and in some depth since the rest of this thesis looks at how their use may alleviate digital evidence's outlined problems:

- Some general ontologies will be first covered because they may provide assistance. Included in this section will be some ontologies relating to the Internet of Things and Building Automation Systems as these arenas also have to contend with the same problems as digital evidence. There may be some lessons that can be learned;

- Specific digital evidence ontologies will then be considered to understand how the field has been advanced and any shortcomings that have been identified; and
- Finally, there will be a summary of the material with a proposal for future work.

This leads to the Chapters 4 and 5 which detail "DESO", the ontology designed to act as a classification system. This ontology is then applied to some digital evidence problems in Chapter 6 to understand how it answers the research questions and identify any shortcomings that require further work.

3.2 Terminology

3.2.1 Models

Whilst the term "model" is liberally used in digital evidence research - examples [11, 21, 197] - the term is rarely defined. Since the authors surveyed do not define the term when using it, the presumption is that reliance is placed on the common perception of the word. Sampled dictionary definitions are in relative agreement:

- "something that represents another thing, either as a physical object that is usually smaller than the real object, or as a simple description that can be used in calculations" [48]; and
- "A thing used as an example to follow or imitate" [185].

Philosophically, Frigg and Hartman [102] note that models can perform two functions. The first can represent a certain section of the world - either the phenomena or data they contain. The second function of a model is its use to represent a theory - representing its "laws and axioms". They note that these functions are not mutually exclusive.

The word "axiom" is used frequently by the model and ontology field. and for clarity is taken to mean, in this context, " a statement or proposition on which an abstractly defined structure is based" [187].

There is no intention to pursue a protracted debate on the issue. It appears that the word "model" is a general term to describe a representation of some sort for others to use.

3.2.2 Taxonomies

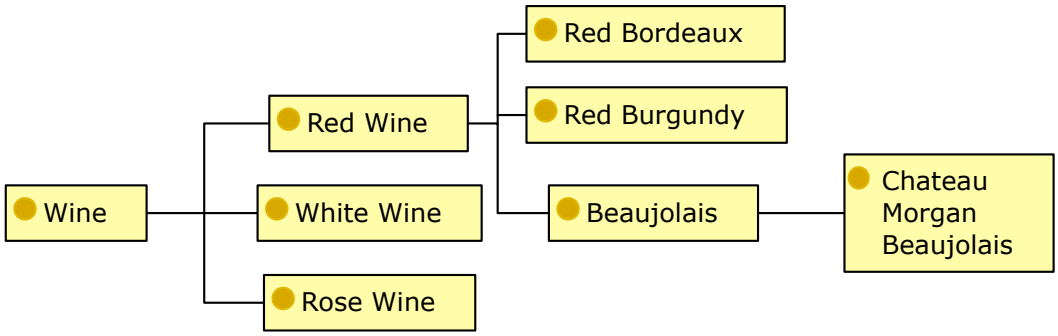

Fig. 3.1 An example taxonomy based on Noy and McGuiness' Ontology 101 [180]

The word "taxonomy" also enjoys a wide use - examples [71, 18, 196] - but, similarly, reliance is placed on the common meaning of the word rather than any explicit specification. Again, sampled dictionary definitions are broadly in accord:

- "A scheme of classification" [186]; and
- "A system for naming and organizing things, especially plants and animals, into groups that share similar qualities" [49].

An example taxonomy is shown at Figure 3.1. Here, the increasing definition of a bottle of wine is shown in a tree structure.

This is useful to put some sort of order on a set of terms but there is a difficulty in representing complexity. If a solution to the research problems involves looking at the situation from more than one perspective, how is this modelled using a taxonomy?

So for example, if the concept to be modelled included not just the classification of the wine itself but also its properties such as "flavour" and "body", how would these be represented?

It is anticipated that the digital evidence concept to be represented will require such a multi-faceted view because the Research Questions cover not just the location of artefacts but also how they can be compared.

This brings the discussion on to ontologies - which allows more sophisticated concepts to be represented.

3.2.3 Ontologies

Whilst original uses of the word "ontology" relate to philosophic fields, it is becoming increasingly exploited in the computing, knowledge representation and artificial intelligence arenas. When using the word in this dissertation, it relates to knowledge representation.

Even within the field of knowledge representation, the word "ontology" has a variety of meanings. For clarity, these will be briefly covered.

Gruber's, now classic, definition of Information System (or knowledge representation) ontologies is that they are an "explicit specification of a conceptualization" [118]. But, in the same paper, Gruber expands this a little further to describe how they are a "representational vocabulary for a shared domain of discourse — definitions of classes, relations, functions, and other objects". Gruber puts forwards a key purpose of ontologies - for the sharing of knowledge.

In explaining "conceptualisation", Gruber states that it is an "abstract, simplified view of the world that we wish to represent for some purpose." [119]

Handler [131] proposes a similarly simple description of ontologies "as a set of knowledge terms, including the vocabulary, the semantic interconnections, and some simple rules of inference and logic for some particular topic".

Chandrasekaran et al [62] describe ontologies as one of two, seemingly interrelated, concepts:

- The first is a representational vocabulary for a specific domain or subject matter. What matters is not the actual terms that are used but the concept being captured. In this way, the terms could be translated from, for example, French to English, and, though the words may change, the concept would not. The authors note the care required in analysing the kinds of objects in the domain and the relations that can exist in the domain studied.

- The second use of the word is, instead of describing a domain conceptually, it is captured as a body of knowledge. Facts take the place of conceptual terms.

Smith [227] puts forward a definition that, for information science, an ontology is "a dictionary of terms formulated in a canonical syntax and with commonly accepted definitions designed to yield a lexical or taxonomical framework for knowledge-representation which can be shared by different information systems communities."

But, crucially, Smith states that an ontology not only has these definitions but also "a supporting framework of axioms". This means that, for this definition, an ontology is more than a taxonomy - it requires statements about the inclusion of entities in classes and the relationships between them. This a view largely echoed by Uschold and Jasper [249].

All of the surveyed sources noted how the use of the word was indistinct - indeed Hendler [131] believes the term has been abused with different meanings ascribed to it by differing communities. There is an irony to this observation in that this ambiguity is actually a key problem that an ontology is intended to solve.

However, there are similarities in definitions: the need for a consensual, community, view; and the need to model a specific domain. But the conclusion from this review is that further discussion of the meaning of the word "ontology" is moot. Instead, it is better to understand how ontological properties can help to address the Research Questions - and then use this understanding to form an ontology as a solution.

The next sections provide a practical illustration of an ontology then consider its uses and how these could assist in answering the Research Questions.

3.2.4 What do Ontologies look like?

Ontologies are a system of "Classes" and "Sub-classes". "Instances" are placed into this system in the same way that sets and subsets have members. The earlier referenced "axioms" are statements governing the conditions that instances must fulfil to be a member of a particular sub-class.

This, alone, might be taken for a taxonomy - as seen in the wine example at Figure 3.1. But an ontology may consist of a number of taxonomies, now renamed "classes". All represent a particular standpoint with "Object" and "Data" properties used to bring further sophistication to the model.

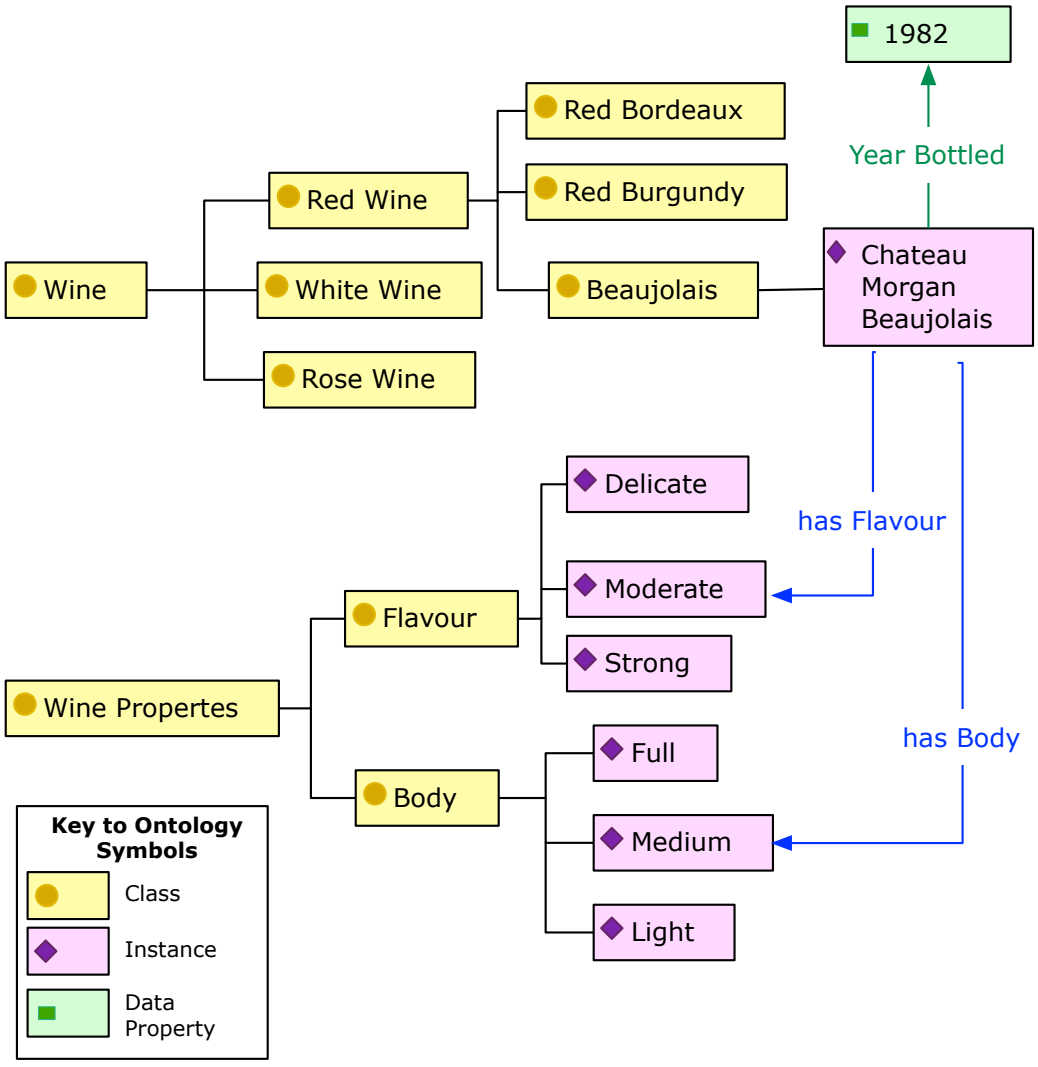

Fig. 3.2 An example ontology based on Noy and McGuiness' Ontology 101 [180]

To illustrate, Figure 3.2 builds on the earlier wine taxonomy at Figure 3.1. It displays two classes (yellow coloured circles): “Wine” and “Wine Properties”. Each have sub-classes.

Instances (purple coloured diamonds) are placed in appropriate sub-classes.

Object Properties (coloured blue) join instances to build up a conceptual picture. They describe relationships between the instances in different sub-classes.

The Data Properties (green coloured squares) are used to add extra description to the instances within these classes.

So, in this example it can be seen that the wine ‘’Chateau Morgan Beaujolais” has a “moderate” flavour and “medium” body. The wine was bottled in “1982”.

As can be seen, this is much more versatile method for describing a particular concept or, in ontological terminology, a “World View”.

3.2.5 What are ontologies used for?

From the varying definitions of an ontology, it logically follows that there are various views on their use. Indeed the self-referencing term “meta-ontology” has been introduced to describe an ontology that describes ontologies.

Whilst helpful contributions are made by Gomez-Perez et al [116], Uschold and Jasper [249] and Gasevic [109], the most accessible description is a guide by Noy and McGuinness [180]: “Ontology Development 101 - A Guide to Creating Your First Ontology”. This implicitly describes an ontology by listing some reasons for creating one:

- *Sharing a common understanding of the structure of information amongst people or software agents*. This addresses a concern raised by Smith [227] who noted a key problem in Information Science: disparate groups have their own idiosyncratic terms used to represent information. Similarly, these groups may use the same terms but ascribe different meanings to them. As more groups wish to share and translate this information, the problems increase “geometrically”. Using the Wine example from section 3.2.4, all vineyards could use the terms to describe their respective wines.

- *Enabling reuse of domain knowledge*. In the same way that functions in a computer program can be reused, the modelling of a domain in a particular sphere can be reused in another. For Digital Evidence, this could be the compilation of an ontology detailing file systems. Originally this could have been used for modelling operating systems but it also could be used for the location of evidential artefacts. Lopez et al caution on re-usability [116, p.34]: the more generic an ontology is made to allow subsequent reuse, the less usable it becomes for the domain in which it was originally intended.

- *Making explicit domain assumptions*. These are, essentially, top-level assumptions about the environment in which a system operates. If all entities in the system

individually use their own assumptions, it can be difficult to effect a change in any environment being modelled. By having a common, upper, reference point used by all entities, any change is easier to facilitate as it can be made at this one level rather than for all of those below it.

- *Separating the domain knowledge from the operational knowledge*. The relates to using functional separations and assigning ontologies to each. As example, an operation could be to turn a water tap on. But the functional separations could include the physical theory on how the movement of the hand can turn a tap on and what causes the water to then flow out of the tap.

- *Analysing domain knowledge*. If an ontology is accurately specified then the domain it covers can be analysed accurately - what it will and will not cover. This allows the effective selection of an ontology for knowledge reuse.

Whilst all of these could be of use in addressing the stated challenges of this thesis, the most relevant are the ability to share a common understanding of an information structure and knowledge reuse.

The first allows the correlation of disparate pieces of information to make links. The second, as earlier alluded, allows for knowledge about, for example, a FAT file system installed on a USB memory stick to be also employed when it is used to assess the same file system on a different device.

3.2.6 Ontological Commitment

An ontological commitment is the shared agreement amongst all users on what that ontology represents. The ontology need not represent everything in each individual sphere but, for all those who subscribe to it, the outlined terms, objects and relations should be consistent amongst them all. This is how a shared understanding for the exchange and reuse of knowledge is reached.

Each party will know different things - the ontology creates a shared vocabulary for the exchange and use of this knowledge.

3.2.7 Design principles for ontologies

Whilst the benefits of an ontology are readily apparent, creating one can be difficult due to the required ontological commitment.

Smith [227, p.159] notes the difficulties of compiling a single shared ontology: the framework must be sufficiently neutral to make it widely accepted by a variety of communities. But to ensure maximum use, there is also a desire for an ontology to be as wide-ranging and detailed as possible. This creates a tension.

To alleviate these problems, ontologies can be composed as a series of layers - a top, “upper”, level to serve as a “common neutral backbone” with more specialised ontologies

below it. In essence, keep the upper ontology simple and high level to allow a maximum number parties to commit. There may be factions of these parties under this level who wish to create and commit to their own ontologies but they will reference the high level ontology that has already been agreed. The lower levels will be subsets of the upper one, not contradictory.

Gruber [119] defined five principles for the design of formal knowledge representation ontologies. These will be covered because they provide a useful check for any Digital Evidence ontology that is developed. These are shown in Table 3.2.7 below.

Gruber's five principles for formal knowledge representation using an ontology [119]

Area	Description
Clarity	Terms used in the ontology should unambiguously communicate their meaning. Definitions should be objective - not tied down to any particulate topic area or use of technology. Where possible, logical axioms (statements) should be used to define the ontology. What is it based on?
Coherence	As a minimum, the defining axioms should be consistent with each other. Also, the conceptual definitions should fit any examples. This means that the best way of testing the ontology is by using it - do the example instances fit into the structure?
Extendibility	The use - and future uses - made of the ontology should be considered. In doing so, it should be kept to a minimum, essential, foundation that allows additional uses to be made of any terms without change to the original structure.
Minimal encoding bias	The ontology should be specified using knowledge, not the technical terms of any particular arena. The reason for this is that the use of these technical terms inhibits reuse by any committed party that does not use these particular terms.
Minimum ontological commitment	Only define the minimum required to allow the required knowledge sharing activities - this is tied in to the facilitation of extendibility

Gruber does, however, note the compromises required when compiling an ontology. The principals are check points to use in the design not hard and fast rules.

3.2.8 Assessment of terms

The definitions of the terms“Model”, “Taxonomy” and “Ontology” are vague. However, the properties of ontologies offer clear benefits in addressing the problems identified in section 1.2. These are:

- The ability to reuse domain knowledge adds an essential extensibility which can be used to cater for an increasing variety of digital devices. For example, if a file system such as “NTFS” is specified in the ontology, any device using this file system can reuse this knowledge instead of it having to be restated for each device in which it is used. Further, if artefacts of a certain type are found to offer assistance in answering a particular investigative question, the ontology can be queried to understand where else these artefacts may also occur? This assists availability and selection and goes some way to answering Research Questions 1 and 2;

- The ability to make domain assumptions assists in building up knowledge. For example, any devices connected to a network using “Ethernet” will have a “Media Access Control” (MAC) address.

- Separating domain knowledge from operating knowledge directly addresses the problems seen with the surveyed forensic tools discussed in Chapter 2. The tools were seen to address the technical aspects of digital evidence - such as extracting internet browsing history - but not the investigative ones - such as did a suspect ever visit a particular location? Instead, the debate has to be abstracted to a different level: first, the prospective 5WH investigative questions have to be considered. But when these questions are decided, they are then overlaid on to the available digital evidence artefacts. In this way only data relevant to the investigation is considered. This approach aids selection and goes to answering Research Questions 3 and 4. Further, properly structured, an ontology will identify all artefacts that can assist in answering a particular question without a deep knowledge of any individual technology.

- Ontologies can assist in analysing domain knowledge: for example, a device is known to be mobile yet there are no listed artefacts concerned with location. This may focus research attention to consider the question: is this because there are no generated artefacts concerning location or have they not yet been identified?

Taxonomies may be too simple a representation to solve the research problems but, in reviewing material, models and taxonomies will be considered as well as ontologies. The reason for this approach is the ambiguity of the terms: there may be models and taxonomies that have ontological properties and can be re-used in any ontology that is subsequently developed.

3.2.9 Basis for review

The basis for the review of models, taxonomies and ontologies is to understand the following questions:

- What is the proposal - what does it purport to do?
- How does it implement this proposal?
- Does it achieve its objective?
- Can it assist in a solution to represent Digital Evidence artefacts in such a way that they can be:
  - recorded;
  - selected based on suitability to a particular investigation;
  - compared; and
  - assessed for their reliability.

3.3 The contribution of models

There are few arenas where every source of potential data can be exhaustively collected and reviewed – this is particularly the case when it comes to the collection of evidence and its examination. For example, at a scene of crime, not every surface can be examined for fingerprints, traces of body fluids or other contact evidence. Instead, there are practical constraints applied relating to the likelihood of evidence being found and, in conjunction with the severity of the crime, the resources to actually conduct this examination.

As previously outlined, this is also true of the Digital Evidence field where the volume of material gathered has dramatically increased. So what should be examined and when? This is the reason for having a digital evidence model – something which can inform the examiner of where to look and in what order so that the most useful evidence is found.

The key models will now be surveyed.

3.3.1 DFRWS 2001

The genesis for a number of early digital evidence models came from research presented at the first Digital Forensic Research Workshop in 2001. It set out to provide a research base for the field of Digital Evidence.

Its conclusions [190] stated that the digital sources analysed to obtain suitable evidence had three things in common:

- “First, they are increasingly complex and less understood overall.

- Second, they are constantly morphing in form and function.
- Third, at the root of all their increasing functionality and detail are fundamental technologies that can be explained scientifically".

This conclusion has stood the test of time however, with regard to the third point, although it remains true, the systems now examined are of such complexity that the scientific explanation of the underlying technologies could well be impractical.

A pertinent paper given at this conference by Eugene Spafford laid the ground work for much of what later models should have been addressing. He commented: "We need to know how much information and what type, exactly, we must collect to afford the most accurate analysis under particular circumstances". This is the selection problem - Research Questions 3 and 4.

This conference also established a Digital Forensic Road Map to: "Define a generic investigative process that can be applied to all (or the majority of) investigations involving digital systems and networks. The Digital Investigative Process (DIP) must be defined from highest level categories to the individual steps necessary for complete analysis of all potential digital evidence."

Whilst this covered a number of issues it did not, in fact, address the comments made by Spafford – essentially, how do you see the digital wood from the trees? Nevertheless, it was the beginning of a digital evidence model.

3.3.2 Stephenson 2002 - 2003

Stephenson, in a number of articles spanning from 2002 to 2003 [230, 232, 231, 233], built on the DFRWS framework - applying it to a methodology named "End to End Digital Investigation" (EEDI).

Even though Stephenson's main thrust is computer network attacks - Incident Response - he still notes that key to this process is the continual cycle of interaction between the digital and traditional investigators - feeding investigation leads back and forth as they are found. A key observation is that "there is no magic program that we can plug our evidence into that automatically extracts just what we need for our case" [230].

For its time, the work is novel but there are no concrete measures in it that could usefully be applied to answer the Research Questions.

3.3.3 Carrier and Spafford 2003

In 2003, Carrier and Spafford attempted to move digital evidence models to a more practical basis [51]. The paper's most pertinent comments are made when discussing the generic model of physical crime scene investigation – as gleaned from a number of published works. The authors comment that "this model allows the crime scene to be thoroughly documented and uses the investigator's experience to find useful pieces of

evidence. Not all physical objects can be taken from the crime scene, so the Search Phase must be thorough enough to gather the needed evidence but not overload the laboratory with unrelated objects."

This recognises the availability and selection research problems but there no proposals to provide any answers to them.

3.3.4 Enhanced Digital Investigation Process Model and Mocas Review 2004

In 2004 the "Enhanced Digital Investigation Process Model" (EDIP) was proposed [21]. The model aimed to "include the physical and digital crime investigations".

The model is a little short on detail - particularly what it calls the "dynamite phases" - the actual analysis of the examined data. This might be considered the most time consuming and difficult aspect of the case. Nevertheless, its suggestion of an iterative approach is useful.

Also in 2004, a paper was produced which recognised the "Investigative Context" [167]. Its desired outcome is "to produce reliable evidence that is useful to an investigation and admissible in a proceeding".

But the paper also discussed "Minimalization" which it defines as collecting and examining the minimum amount of data. This is Research Question 3 but there are no suggestions that would assist in answering it.

That year also saw the publication of a survey on computer forensics [208]. The survey found that there was "disproportional focus on the applied aspects of computer forensics, at the expense of the development of fundamental theories".

As this survey of digital evidence models progresses, it is apparent that very few of the, often most erudite, proposals have come into main-stream use in the digital evidence fields. The reason for this is considered at the end of this section.

3.3.5 Ruibin 2005

Ruibin et al [214], puts forward the term "case-relevance" - defined as a measure of any piece of information's ability to answer the investigative "who, what, where, when, why and how" questions in a criminal investigation".

In this way, the technical data is used most appropriately to answer the investigative questions. The proposed model, is an early suggestion of "Predictive Coding" - see [204] - used for E-Discovery. Essentially, fundamental or "seed" keywords are chosen by investigators then fed into data. Results are then assessed using machine learning against stipulated objectives.

Though the model is no more than a sophisticated implementation of keyword searching - with attendant drawbacks previously discussed - the suggestion of applying the 5WH concepts to technical investigation is useful.

3.3.6 Beebe and Clark 2005

Instead of a model, Beebe and Clark in 2005 [25] proposed a "framework" incorporating phases, sub-phases, principles and objectives.

They argue that "a digital investigation framework must be based on objectives, rather than tasks". It is the first paper noted that discussed a matrix of tasks and objectives. The reason for this format is that the relationship between the two is not linear – ie one task can accomplish a number of objectives and in attempting to achieve an objective, there may be a choice of a number of tasks.

In illustrating this approach, they suggest how it is easier for an examiner to decide if an enquiry is relevant by referencing it as "Determine whether unauthorized software has been installed" as opposed to "Examine the Registry". This is the same topic as addressed by Research Question 4.

Their "Data Analysis" phase aims to answer the 5WH questions. To perform this role, the task / objectives matrices are employed to marry to allow "the digital forensic examiner to quickly determine which objectives and in turn which specific tasks are applicable to the incident and approach strategy at hand."

This is an interesting concept but it still does not assist with availability or selection - it just allows easy recall once the mapping of tasks and objectives has been decided. Further, the use of a matrix may not easily allow for change - either in the complexity of investigative objectives or technology. Rows and columns would require frequent modification.

3.3.7 Politt 2008

Pollitt's 2008 research [196] contends that previously developed models contribute to the notion that all evidence must first be acquired and then the generated material handled in two ways: devising ways to reduce it - for example by removing operating system files - and finding ways to select it, for example, by keyword searching. Both have drawbacks: the first may not sufficiently reduce the volume. The second relies on the examiner being sufficiently well informed on the material sought. Instead he applies four processes to digital evidence examination to improve this approach.

The first, "*Identification*", aims to cover the gap between the investigative and digital demands of a case - the translation from one to the other. He proposes that the process is best approached by first considering the desired information before its possible forms and where it might be stored. Only then is the selection of the tool and query to extract this data in the desired locations. In a sense this echoes Beebe and Clark's [25] idea of setting questions based on the required information rather than the specific technical task.

Pollitt justifiably contends that this approach reduces the burden on the examiner and produces relevant evidence. This is key to Research Question 3.

The second, "*Classification and Individualisation*", aims to mimic the processes in other forensic disciplines such as ballistics - covered earlier at Section 2.4.2. The disparate artefacts can be composed to form a picture of characteristics - which can then show that that an object or certain data is either representative of a certain class or of a unique identity. This is the correlation research problem.

The third, "*Association*", relates to the traces left when an event happens - such as the insertion of a USB memory stick into a computer. For digital evidence, Pollitt emphasises the necessity of noting what artefacts can be compared and where they are located. This contributes to the selection of evidentially "Rich" data from "Identification". This is the Principal Research Question 1.

The fourth, "*Reconstruction*", looks to put any identified events in some sort of order to gain a clear picture of what happened.

Pollitt makes a case that legal and investigative questions must be defined before defining any digital forensic questions.

From these proposals, there are no suggestions of how they could be implemented. However, the principal is carried through to the design of DESO and how it is used to select artefacts based on the needs of the investigation.

3.3.8 Hunton 2010

In a series of papers Hunton develops the "Cybercrime Execution Stack" and a model for Cybercrime investigation [137–140].

Hunton's definition of cybercrime is wider than criminal activity - also encompassing the generic "harmful behaviour" - but restricted to actions assisted or enabled by technology. This does not encompass events where technology acts as a "witness" to events such as a suspect being placed at the scene of the crime by their mobile phone's location.

The proposals act as useful model for how the defined "cyber crime" can be committed and then investigated. However, it is purposefully designed as being high-level and, from this perspective, the model and investigative framework offer no assistance when addressing the research questions. Where they may be of use is in providing an overall guide - perhaps being applied onto any solution that is found for these challenges.

3.3.9 Contemporary models

Smith and Petreski [228] propose an index to determine the best method for investigating the technological elements of a case. This is based on such metrics as "effectiveness", "Level of effort" and "Compatibility of toolsets".

Whilst this is applied to sample cases, the difficulty with these metrics is that they assume criminal investigations to be constant or predictable. As discussed in section 2.1, they are not. Nevertheless, if such metrics could be kept and applied, it may be possible to

see if the same techniques are effective regardless of the investigation. This is beyond the scope of this dissertation but may prove useful further work.

Raghavan et al's model [202] proposes time lining as a way of addressing volume and variety. The drawbacks of time lining have been covered earlier at Section 2.9.5. Without a method of locating and selecting the correct time artefacts, this approach is unlikely to succeed as, first, some vital points of data may be missed and, conversely, there may be too many irrelevant time instances to discern any pattern or illuminating sequence of events.

Bulbul et al [44] offer a comprehensive view on the digital evidence crime scene - noting how the recovered digital evidence must be tied into any physical evidence. However, they do not focus on identifying, extracting and comparing artefacts so this research is not able to offer assistance.

Most recently, in 2017, Amato et al [8] outlined the problems addressed by this thesis and propose the use of ontologies which are then queried. But aside from these suggestions, there is insufficient detail to assess their approach. No ontology is specified.

3.3.10 Summary

Two general types of models were found: those that guide the digital evidence examination process and try to solve the case and those that model data and allow other tools / humans to draw conclusions.

But in terms of addressing the problems addressed by this thesis and resulting Research Questions, there were few found to be anything other than meta-solutions - those advising on what a good solution should look like without a practical proposition.

The study will now move on to ontologies and taxonomies to understand what can be learned from this particular area.

3.4 Selected ontologies indirectly related to Digital Evidence

3.4.1 The Gene Ontology

The Gene Ontology proposed by Ashburner et al [16] was developed as the fields and genetics and bio-chemistry realised that there was a finite universe of genes and proteins. The knowledge of the biological role of one protein in an organism can allow conclusions to be drawn about the role of other organisms when the protein is also present in it.

But the way in which these shared biological elements were being described and organised was not sufficient to keep pace with the rapid discoveries emanating from genomic sequencing. Different fields of study had varying methods of describing a protein and its function. This meant that the transfer of knowledge — such as the role of a protein - was not taking place. This required a shared vocabulary so that a protein recognised in

one field of study was linked to its presence in another. And with this, the observation of the protein's role in one field could be used in the other.

A key requirement of this vocabulary was to cater for the need to "organise, describe, query and visualise biological knowledge at vastly different stages of completeness. Any system must be flexible and tolerant of this constantly changing level of knowledge and allow updates on a continuing basis."[16]

Four years after this initial description, in 2004, Harris et al [111] reported on a, now viable, and active ontology that was used by the community. The three goals were to:

- Develop a set of controlled vocabularies (the Gene Ontology) to describe key domains of molecular biology
- Use the terms in this ontology to annotate genetic material and behaviours in biological databases
- Provide a central public resource allowing universal access to the ontologies and annotation data sets in addition to the tools for use with this data.

Each Gene Ontology term has a name and a unique alphanumeric identifier. Consortium members of the Gene Ontology submit annotations about various gene products by citing:

- The reference used to make the annotation - such as a journal article;
- An evidence code indicating the type of evidence upon which the notation is based; and
- The date and creator of the annotation.

The principles of the Gene Ontology are directly applicable to the Research Questions addressed by this thesis for the following reasons:

- it provides a method for documenting genetic data. This could help to answer the principal Research Question 1 and Research Question 2 relating to availability;
- its method for documenting characteristics to allow comparison could be used for Digital Evidence - if properly considered. This helps to answer Research Questions 4 and 5 relating to selection and correlation; and
- the quality of evidence supporting assertions about these artefacts can vary - from a blog with no supporting data to a paper in an authoritative journal with supporting data and details of experimental data. The Gene Ontology - using its evidence codes can cater for this variety. This assists in answering Research Question 7 relating to reliability.

3.4.2 Recording of provenance

Bibliographic ontology

The Bibliographic Ontology [80]is a conceptual representation of the reference sources typically found in academic material such as this thesis. It can be used as an ontology for citations, document classification or to describe any kind of document in Resource Description Framework (RDF) [40].

Amongst its terms, data and object properties its only contribution to an online presence are the classes for "website" and "webpage". This does not cover delineations such as "blog". Since this is a relatively current version of the ontology - produced May 2016 - it is not clear if this is an omission or, simply, that it was felt any lower level of detail is unnecessary. This latter point is a viable argument since terms such as "blog" are indistinct. The base requirement is for a user is to know the URL where this source can be found and the date of access.

Further detail is required on the type of material published - not its location. For instance, is the published material the lone musings of a researcher or a detailed description showing full workings and test data? The Bibliographic Ontology does not assist with this but the Evidence and Conclusion Ontology can. This will now be detailed.

Evidence and Conclusion Ontology

The Evidence and Conclusion Ontology (ECO), as described by Chibucos et al [64], documents evidence found during research and the assertions that can be drawn from it.

The ECO was primarily formed to support the Gene Ontology. As with the digital evidence field, the study of life sciences uses a wide variety of techniques and tools to generate data. From this evidential data, assertions are made and conclusions drawn. As noted when discussing the Gene Ontology, the conclusions from a certain genomic sequence may have relevance where the same protein is found in a different organism. Conclusions can be published, for example, in a journal, conference paper or online.

The ECO's purpose is to document the type of evidence generated and the assertion method:

- The type of evidence can be documentation of the experiment type. For example, "competitive growth assay evidence" which is described as "A type of biological assay evidence in which a mutated strain of a microorganism, such as a yeast or bacterium, is grown competitively with wild-type cells and the relative fitness of the strains is assessed."

- The assertion method documents how the Gene Ontology entry was devised. How does the evidence support it? This can be "manual" - where the material was generated or reviewed by a human. But it can also be "automatic" where it has not been reviewed by a human but is automatically inferred - possibly by some sort of

algorithm. For the Digital Evidence field this latter assertion type could be applying an assertion about a Windows 7 operating system artefact to Windows 10 if the program code has not changed.

Though there is now consideration being given to widening the scope of the ECO beyond life sciences and the Gene Ontology [95], most of its current manifestation is quite specific to that field.

However, there are parts that are immediately applicable to any proposed solution - for example:

- the class "traceable author statement used in manual assertion" references statements that are attributed to a cited source; and
- the class "inference from background scientific knowledge used in manual assertion" is defined by the ECO as a "curator inference that links the current annotation to a different evidence-based annotation via background knowledge of the curator." Again, this could allow for a particular property seen in an operating system to be also linked to a subsequent Service Pack

A key point to note about the ECO is that it is not looking to filter out "good" and "bad" annotations. Instead it is looking to accurately document the provenance of them. How much reliance can be placed on them?

The PROV ontology

In a similar vein to the ECO is the PROV ontology [157] - explained by Moreau et al [169] - which provides a set of terms to describe how data or "things" were produced. This can encompass entities, activities or people and allows an assessment to be made on the data / thing's "quality, reliability or trustworthiness".

There are six components including:

- entities and activities - including the time that they were created or used - this could include a forensic tool or a reference source used for the interpretation of data;
- derivations of entities - this could allow for the extraction of, for example, a file from the the image of a hard disk - which itself is a derrivation of the data on the physical computer hard disk; and
- a method for aggregating provenance records together to provide information on a particular item of data.

Object properties, such as "prov:wasGeneratedBy" allow the link to be established between data and the entity or activity that created it.

The PROV ontology is a comprehensive W3C standard that could be used to document the chain of evidence from an item's initial seizure to the presentation of some arcane

derived data. Further, it documents how the cited source supports the creation of the data - for example "prov:qualifiedAttribution" and "prov:wasInfluencedBy". But where it does not assist is in documenting any perceived quality of the sources themselves.

Both the ECO and PROV ontology could provide useful methods for describing the process by which digital data is transformed from the initial collection to its subsequent derivations and interpretation. PROV is more aligned with the chain of evidence whereas the ECO is more useful for interpretation. And it seems sensible to use one or more of these to document provenance rather than a novel solution. Ontological reuse is, first, more efficient and, second, allows the use and sharing of knowledge with other fields.

3.4.3 The Recording of Time

The Time Ontology [74] has been developed to provide a uniform understanding and representation of temporal references in web pages or, indeed, anything that can be referenced using a Uniform Resource Indicator (URI). This includes the various components of an ontology.

This is a relatively mature standard with the first draft put out for comment in 2004 [134] and it now falls under the stewardship of the World Wide Web Consortium (W3C).

The Time Ontology provides little obvious assistance in answering the Research Questions but, should any time references be required, then there seems no reason not to use the terms specified in it. This leads to reuse with other ontologies and interoperability. Of particular use is "https://www.w3.org/TR/owl-time/#time:Instant" which can be used for the describing and correlating the various time stamps that are encountered.

3.4.4 The Internet of Things

The Internet of Things (IoT) also has to address the same challenges as the Digital Evidence problems now being studied: the scalability and heterogeneity of IoT components [126]. Two ontological approaches to these challenges will be covered.

Hachem et al [126] describes the devices of the IoT and their function. Three ontologies are used to represent:

- actual physical devices;
- abstract functionality; and
- an estimator - mapping the physical devices on to these functionalities.

From a digital evidence perspective, this could be mapped on to: the digital data itself; the artefacts that are useful to an investigation; and a mapping of these artefacts on to available data. But from this 2011 proposition, it was not possible to find any further development.

But the second ontological approach, the Federated Interoperable Semantic IoT Testbeds and Applications (FIESTA) project [98], is advanced. This is an EU project providing real-life generated IoT test data to researchers from various geographic locations in the EU.

To enable this, an ontology is required so that there is a common consensus on how to describe and represent the measurements from the various sensors attached to the IoT devices. There have been previous instantiations including the Semantic Sensor Network (SSN) ontology [252] but a version for this project is the Unified IoT ontology [4] and its "lite" version submitted to the W3C [30]. Inspection of the ontology shows it to be a comprehensive functional description including classes such as:

- "Device" - with subclasses such as "ActuatingDevice" and "TagDevice";
- Domains of interest - such as "Health" and "Tourism";
- "Sensor" with subclasses such as "CholesterolSensor" (which is also in the Health domain) and "FuelLevel"; and
- "QuantityKind" with subclasses such as "Cholesterol".

Object properties, such as "hasQuantityKind", link "CholesterolSensor" with "Cholesterol" to allow reporting of measurements.

There is a development and organisational commitment for IoT ontologies which is not seen when those for Digital Evidence are later reviewed in section 3.5.

Further, as the field of Digital Evidence expands to include data from IoT devices, it would be sensible to ensure that any Digital Evidence ontology that is developed has the capability to link with the IoT ontologies. This will allow the ready dissemination and inclusion of data between the fields.

3.4.5 Building Automation Systems

Allied to the IoT are Building Automation Systems (BAS) - the various sensors and controllers installed in large buildings to control such facilities as fire alarms, access control, heating and ventilation. Though not necessarily connected to the Internet, these are similarly large systems involving the assimilation and interpretation of data from disparate heterogeneous sources.

Charpenay et al [63] reported on "Project Haystack" in 2015. A series of ontologies were introduced for tagging various BAS components and creating domains such as air, water, humidity and temperature. Reasoning can then take place using these ontologies to control the BAS functions.

A check of the current project website [199] shows Haystack to be a trade association comprising at least 24 members with open source specifications available for download.

Making use of Project Haystack's tags is "Brick" [19] - which attempts to advance the field of BAS. It does this by defining a core ontology of fundamental concepts and their relationships which is allied to domain specific ontologies covering specific building concepts.

Brick is reported as having been implemented on six buildings and found to work well using the "notion of synonyms to equate sensors and subsystems similar in function" [19].

3.4.6 Observations from non-Digital Evidence related ontologies

The examples of non-digital evidence ontologies show well-developed concepts that could be of use in any solution.

In particular, IoT and BAS ontologies that have already been implemented show that it is possible to unify measurements from disparate systems. If forensic tools are equated to these measuring systems, then an appropriately framed functional ontology could provide the same role.

Further, the BAS and IoT fields show that it is possible to obtain ontological commitment that allows the sharing and reuse of knowledge.

Finally, when other forensic fields were surveyed in section 2.4.4, the role of government or non-commercial bodies was necessary to form standards for inter-operability. But the Project Haystack project in the field of BAS has shown that the private sector is quite capable of solving these problems. And this field is not alone: the USB Implementers Forum [248] and GSM Association [121] are two examples of industry bodies setting standards that are in world-wide use.

3.5 Digital Evidence ontologies - summary of findings

A total 24 ontologies and taxonomies covering the digital evidence field have been surveyed. These were published between 2006 and 2017. For readability and brevity, the full listing of those surveyed and a summary of their capabilities is included at Appendix B.

The sample of 24 were assessed on:

- the problem they were looking to address;
- their stage of development;
- their effectiveness in addressing the stated purpose; and
- their ability to assist with the Research Questions.

Findings are as follows.

3.5.1 General immaturity

As noted at section 3.2.3, the definition of the word "ontology" is broad and unspecific. However, only ten of the surveyed 23 ontologies went beyond description of a concept to describe even a light ontology such as, for example, a class system. Fewer still provided further detail such as object and data properties or broader axioms.

3.5.2 Lack of reuse or commitment

Material introducing the ontologies, such as published journal papers, made reference to previously outlined ontologies - for instance Harrill and Mislan's "Small Scale Digital Device Forensics Ontology" [128] was commonly cited. But, aside from Schatz [217] there were few examples of ontologies making use of pre-existing work - or indeed, ontologies from other fields. This does not take advantage of one of the key benefits of ontologies as stated by Noy [180]: reuse of domain knowledge.

Related to this is the isolation of these ontologies. There was no evidence of the multi-party efforts earlier outlined for other fields such as genetics, the IoT and building automation. Instead, the ontologies were developed by a small group without reference to others.

This risk of this approach is that there is a lack of ontological commitment - as outlined at Section 3.2.6. This has an impact on another of Noy's outlined benefits: sharing a common understanding of the structure of information amongst people or software agents.

If the ontology is only developed by a small group without reference to others, this shared understanding is jeopardised and the lack of commitment makes ontological success less probable.

3.5.3 Assistance with the Research Questions

Of the 24 surveyed, only four ontology proposals were able to offer substantive assistance with the Research Questions. The remainder either did not have a suitable capability or provided insufficient detail on which to make an assessment.

Alzaabi et al's [6] ontology for smart phones is of use if the common terms outlined for this environment are applied to other devices and environments.

Dosis's series of lightweight ontologies [83] could assist with availability if they could be used to target specific elements within a source instead of all the data. However, no assistance is provided in the selection of these elements.

Chabot's work on time-lines [60] could assist by specifying a common format for reporting data from disparate heterogeneous sources.

Nimbalkar's work proposed how log files can be interpreted [179]. This is an interesting approach to correlation but one which concentrates on low level data interpretation in a file not any higher level semantic meaning.

3.6 Summary

In chapter 1 the problems facing digital evidence were set out and a series of research questions were posed. In chapter 2 a model or ontology was proposed as a solution.

In this chapter, existing digital evidence models and ontologies have not been found to provide assistance in this regard.

Some of them have sought to view the Digital Evidence field from a "real-life" view rather than conceptually. As example Harrill's Small Scale Digital Device Forensics ontology [128]; Craiger's Digital Evidence Markup Language [75] and Cosic et al's Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence [72]. These approaches model the evidence from the perspective of the device upon which it is contained.

This is a valid ontological approach and may be the most appropriate for the purpose intended by the authors. However, for the purposes of this thesis, the approach has limited value. In attempting to model technology rather than evidence, as the amount and complexity of these increase, any ontology would have to linearly scale in line with the these increases. This is irrespective of the evidential artefacts that they contain.

A different approach would be instead to solely model the artefacts that are required for an investigation and only document the locations where these artefacts can be found. Kahvedzic [147] touched on this point when defining "Evidence Location" in the Dialog ontology.

Whilst existing Digital Evidence models and ontologies do not offer substantial assistance, other fields covering Genetics, the Internet of Things and Building Automation have shown how it is possible to:

- Functionally describe a domain concentrating only on the elements that are required;
- Map these functional descriptions on to individual lower-level domains to create synonyms between disparate systems; and
- Obtain ontological commitment in a community to allow the success of these ontologies.

If a similar system could be developed for digital evidence then the tasks could be addressed as shown in Table 3.6.

Assistance Provided by an Ontology to Solve the Research Problems

Research Questions - as set out in Section 1.2	**How an ontology addresses this problem**
Allow for differing digital sources and the rapid changes in technology	An upper level functional ontology could provide a framework linking new instances of existing and emerging technologies together. The various domains could reference this ontology.
Reduce the volume of digital evidence that requires examination Allow the selection of artefacts based on investigative criteria as opposed to technical ones.	A functional ontology could include only artefacts - data of use to an investigation - not attempt to map the whole system. This reduces the volume that must be addressed. If this ontology was aligned with investigative objectives, then relevant selections could be made.
Allow for successful comparison of artefacts irrespective of their source or originating format	The ontology creates the “synonyms” that allow artefacts from disparate sources - but which the mean the same thing - to be identified and compared.
Allow the use of any tools to process evidence	Any digital evidence tool could make use of this functional ontology to understand where artefacts may be located. It can also provide a reference for the correct format to describe and report an artefact. Ontological commitment creates this shared understanding and allows interaction of the various tools. Developers can specify the functions that their tool can perform.
Provide a system for the provenance of these artefacts to be established	Ontology reuse allows one or more of the provenance ontologies to be used to describe the origin of the information behind any artefact and document its relevance and accuracy.

To address the outlined gaps, this thesis documents research compiling the Digital Evidence Semantic Ontology (DESO). This is documented in Chapters 4 and 5 and then tested in Chapter 6.

Chapter 4 provides a general overview of DESO before looking at the documentation of Digital Evidence artefacts. This is Research Question 2 relating to availability. It will be shown how the proposed ontology allows for differing digital sources and rapid changes in technology.

Chapter 5 documents a classification system for these artefacts that addresses Selection and Correlation - Research Questions 3 to 6. It also shows how the reliability of each artefact can be assessed by documenting provenance - Research Question 7.

Chapter 6 applies DESO to a hypothetical investigation to understand how it assists the process and where there are gaps that require further research.

Chapter 4

The Development of DESO - Structural Overview and Addressing Availability

4.1 Introduction

This chapter introduces the Digital Evidence Semantic Ontology (DESO). First, the research methodology is outlined followed by a brief review of approaches that were not successful with lessons learned. These findings were carried through to the development of DESO, which is then detailed.

The description of DESO first, covers the conceptual background of the ontology's three classes. As appropriate, other aspects are introduced. These include the use of data properties at Section 4.5.3 and the placing of instances, at Section 4.5.8.

4.2 Research methodology

4.2.1 General Approach

DESO was developed organically. It started from the research problems - that an artefact would need to be identified, selected, compared and assessed for reliability. This led to the hypothesis that three classes could be created which would, respectively, describe the location of an artefact, its type and its provenance.

This was applied to test data and DESO was adjusted as shortcomings were identified. The Research Questions from Section 1.2 were used to assess these solutions. These are repeated for easy reference:

- **RQ1:** Can a classification system be devised that allows for the documentation of digital evidence artefacts and facilitates their extraction and comparison?
- **RQ2:** How can this classification system allow for differing digital sources and rapid changes in technology?

- **RQ3:** Is it possible for this classification system to reduce the volume of digital evidence that requires examination?
- **RQ4:** Can this classification system allow for the selection of artefacts based on investigative criteria as opposed to technical ones?
- **RQ5:** Can the classification system allow for successful comparison of artefacts irrespective of their source or originating format?
- **RQ6:** Can the classification system allow the use of any tools to process evidence?
- **RQ7:** Can the classification system provide for the provenance of these artefacts to be established?

4.2.2 Test Data

A sample scenario was chosen: the connection between two different computers when the same USB memory stick is inserted into both. To provide richness to the data, one of these used the Windows operating system whilst the other used Apple's OS X operating system.

This is not a particularly complicated scenario - involving neither great volume or variety of Digital Evidence. However, as stated in Chapter 1, this thesis contends that volume and variety are not the key problems for Digital Evidence but, instead, aggravating factors.

The chosen scenario generates a controlled set of well known artefacts for initial testing. If the Research Questions are answered, more complexity can be added to stress test it.

The method for creating the test data is detailed at Appendix A. A literature review was then conducted with the aim of identifying possible artefacts that would be created by the respective operating systems when a USB device is inserted.

The literature review and the test data complemented each other. The artefacts identified in the review could then immediately be observed in the actual data for confirmation. Often, the location of an artefact was found to be poorly specified in the reference material.

The test data also allowed the use of various forensic tools to understand how they represented the artefacts. This will be detailed in Chapter 6.

As development of DESO progressed, a device running Apple's iOS operating system was introduced to further test the ability of DESO to answer the Research Questions.

4.3 Alternative approaches that were not successful

Before DESO's current manifestation, others approaches were attempted. These will now be briefly covered for the benefit of others addressing this topic.

4.3.1 Linear listing of artefacts

In considering how to list the location of artefacts, the initial approach was to use the ontology class system to mimic the relevant file system. So, for example, an artefact located in the file path \Windows\Documents and Settings\User would be represented by the ontology class structure shown in Figure 4.1.

But this approach does not scale: as file structures become increasingly complex, so the structure of classes and subclasses becomes increasingly verbose - making any class structure unwieldy and hard to read.

The questions to be considered are: how much information does the examiner need to know when choosing a source of artefacts; and is the file path relevant to this choice?

The proposition is that the level of detail only needs to be that required to delineate one source of artefacts from another. This does not have to be, for example, the complete path of folders and sub-folders in a file system.

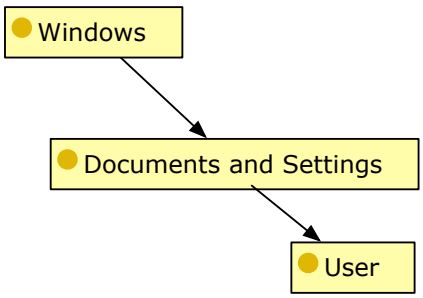

Fig. 4.1 File path represented as a class structure

4.3.2 Artefacts as classes

Another early idea for DESO was to capture the location of all artefacts as a class structure. This was an attempt to apply the principles of the "Photography Ontology" [85] to the world of Digital Evidence. This is represented in Figure 4.2.

The approach moves away from representing the file path as the class structure - as described in Section 4.3.1 and, instead, into categorisations such as "Operating System Artefacts". But, again, this raised a number of problems:

- The Class structure becomes complex because there are many artefacts. This complexity will increase as further artefacts are documented.
- The classification of artefacts is represented from a verbose technical standpoint. Note the entry in Figure 4.2 for "Registry" to the left-hand side of "Windows XP". This may be of little relevance to the examiner whose only questions to be answered are: "What artefacts may exist on the device being examined, which ones do I need and how do I compare them?" As such, the classes are over specified.

- The class system relies on one to one explicit connections between artefacts in different locations. As example, note the connections to "Volume Serial Number" to the right-hand side of Figure 4.2. When a new artefact is added, all existing entries have to be considered to understand whether a connection from them to the new artefact can be made. This will have to be manually calculated and added. A time consuming process that is prone to error. There needs to be a simpler way of making connections across large number of artefacts from disparate sources. The aim is to, effectively, normalise the structure.

4.3.3 Lessons learned

From the previous attempts at a solution it became clear that:

- Attempting to organise artefacts from a specifically technical standpoint makes for complicated class systems. This makes the representation of available artefacts complex and there is no means of selection. Any ontology must be carefully considered for the concepts that are to be captured not the technology that is encountered.
- A single class system representing all artefacts and explicitly listing the connections between them causes complexity and is difficult to sustain effectively. Any ontology must use a process where connections between artefacts can be made without them having to be explicitly defined.

4.4 Introduction to the Digital Evidence Semantic Ontology (DESO)

4.4.1 DESO's basic structure - the concept it captures

The concept represented by DESO is a representation of available artefacts on a given evidence source in such a way that they can be selected for investigative purposes, compared and assessed for reliability.

It is not a view of all the technical data on a device but only those that could have a demonstrable impact on an investigation.

So instead of having a model to represent data on a system, it is a forensic investigation model on to which system data is placed. In this way the collected data is controlled and organised so that it is all potentially useful to an investigation.

To do this, the criteria necessary to capture the "complete" artefact are considered: how can a piece of data be located on a source, what does the data represent and what is the justification for making these assertions?

The three classes of DESO are shown at Figure 4.3:

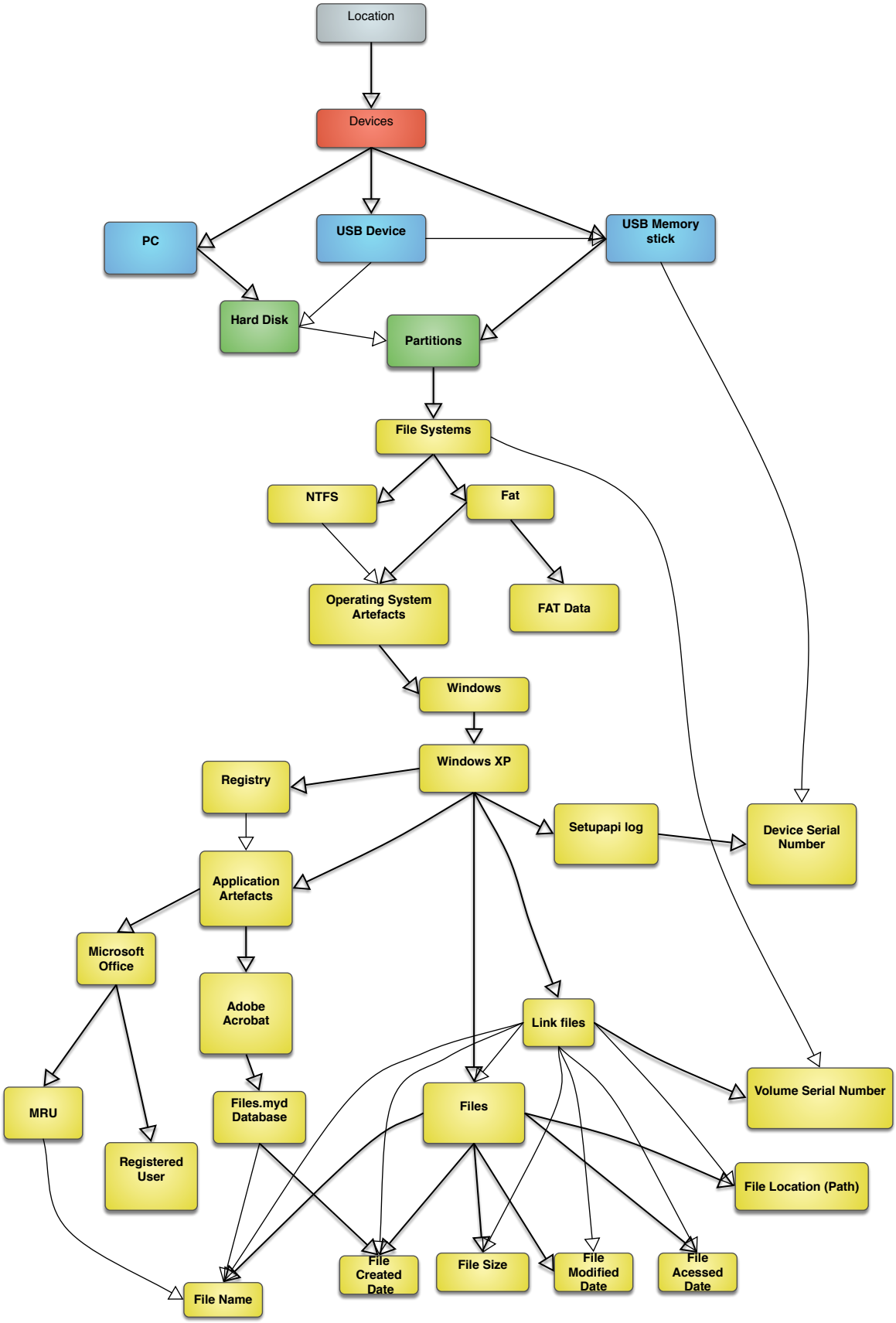

Fig. 4.2 A representation of artefacts as classes. Note the complexity as the various subclasses start linking to each other.

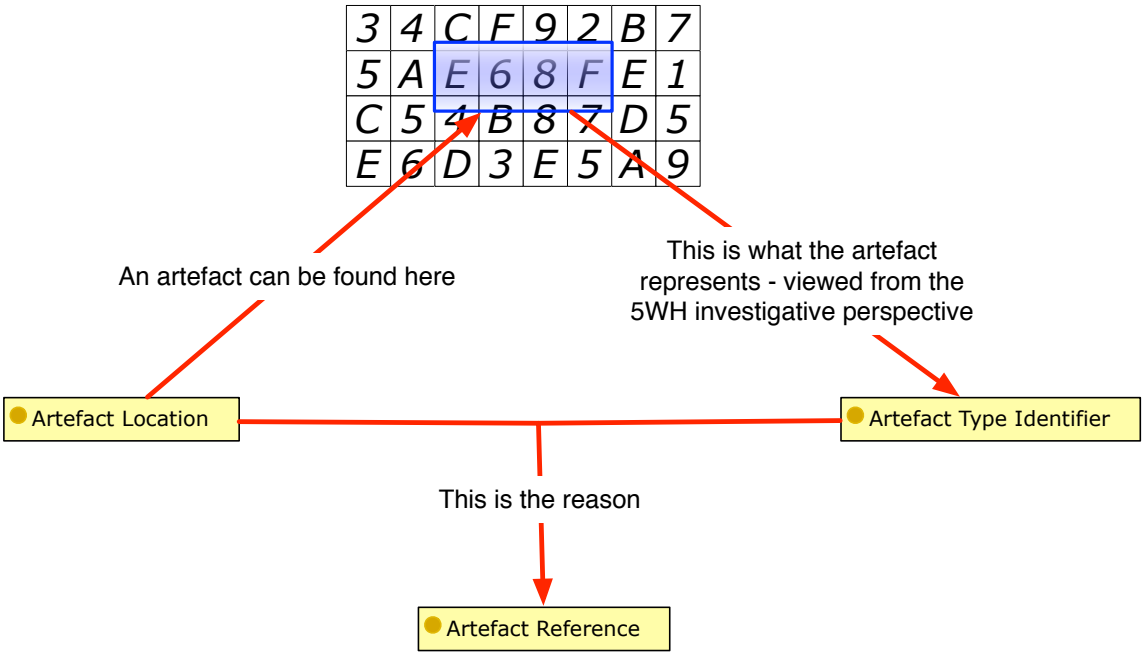

Fig. 4.3 The three classes of DESO

- Artefact "Location" represents the places in digital material at which evidentially useful data can be found.
- Artefact "Type Identifier" represents the meaning of the data at this location - examples of this are a device serial number, a mobile phone IMEI or a GPS location.
- Artefact "Reference" is the reason why it can be said that the data in the stated artefact Location can be classified as a particular artefact "Type Identifier" - this could be an article in a scientific journal, a description in a blog or a technical manual.

A key concept for the artefact "Type Identifier" class is its fundamental structure: the entries are organised using the investigative What, Where, Who, When, Why and How concepts. In doing so, the identification and comparison of suitable artefacts is driven by the needs of the investigation - not the technology.

4.4.2 The necessity for the three classes

Location

First, all data on digital devices are, by their very nature, just strings of ones and zeros. It is the interpretation of these ones and zeros that make these data useful. The location of data within a particular file and, sometimes, the location of the file itself are one of the key descriptors that differentiate one set of digits from another.

Second, unless the location can be adequately described, then it will not be possible for a different examiner to find these data.

But if the location of the data is effectively described then this directly goes to solving:

- the availability problem, covered by Research Question 2 because the artefacts on a particular evidence source are readily identifiable; and
- part of the selection problem relating to Research Question 3 - the ability to reduce the volume of data that requires examination. Only the data at a specific location requires examination, not all of it.

A suitable class structure should allow an examiner to understand what artefacts may be available on the various data sources - either those items already submitted for examination or sources from which data can be subsequently collected - such as a system log file or WiFi hotspot.

Type Identifier

As earlier discussed, a digital device stores and manipulates binary digits. To create any use from them, a meaning has to be assigned to the data at a certain location. Otherwise, the data is just that and of little use to an investigation.

Unless there is a consistency to these meanings, then comparison becomes impossible - the artefacts at different locations remain, simply, disparate pieces of data.

But if this meaning is assigned a Type Identifier and it is consistently applied across all data where it is found, then it goes to solving:

- the remaining part of the selection problem, Research Question 4 relating to the selection of artefacts based on investigative rather than technical criteria. Instead of having to examine all data, the examiner can now be judicious in choosing only the artefacts of a particular Type Identifier that are relevant for a line of enquiry; and
- the correlation problem, Research Question 5, because artefacts of the same type can be compared irrelevant of where they are located.

Reference

To create evidential credibility, there must be a stated reason why it is being asserted that the data at a defined location has a defined meaning. If no reason is provided then other examiners, and any judicial hearing, cannot assess the evidence's reliability. This risks the weight that is assigned to it or, even, its non-admission. This is the reliability problem - Research Question 7.

4.4.3 Overview of how the classes interact

To demonstrate the operation of DESO, two simplified artefacts will be considered:

- A journal paper has documented how a laptop Network Interface Card has a MAC address
- A blog has documented how a wireless access point captures MAC addresses of computers in its vicinity

With reference to Figure 4.4, the addition of artefacts to DESO will be described. For each artefact:

1. The artefact location is considered and an instance created in the appropriate Location sub-class.
2. The Type Identifier is considered and a link made to the appropriate instance in the relevant artefact Type Identifier sub-class.
3. A link is made to the appropriate instance in the relevant Artefact Reference sub-class.

Note how the two artefacts have their own respective Locations and References but share a common Type Identifier. This means that:

- Both artefacts can be located
- The reason for asserting both the Location and Type Identifier is known
- Data extracted from these two locations can be compared because they are of the same type.
- If an examiner is looking for a certain type of artefact, then the locations of that type can be found by tracking back from the relevant Type Identifier instance to the locations that point to it.

Having outlined the basic structure of DESO, the three classes will be detailed and the associated data and object properties will be outlined.

4.5 The Artefact Location class

4.5.1 Structure

As earlier stated at Section 4.4, a design principal of DESO is not to represent all technical data on digital devices but only those that are useful for investigations. This is particularly relevant when documenting the location of files.

At Section 4.3.1 it was shown how merely replicating the file structure as an ontological class caused problems due to the complexity of modern file systems. This caused a complex

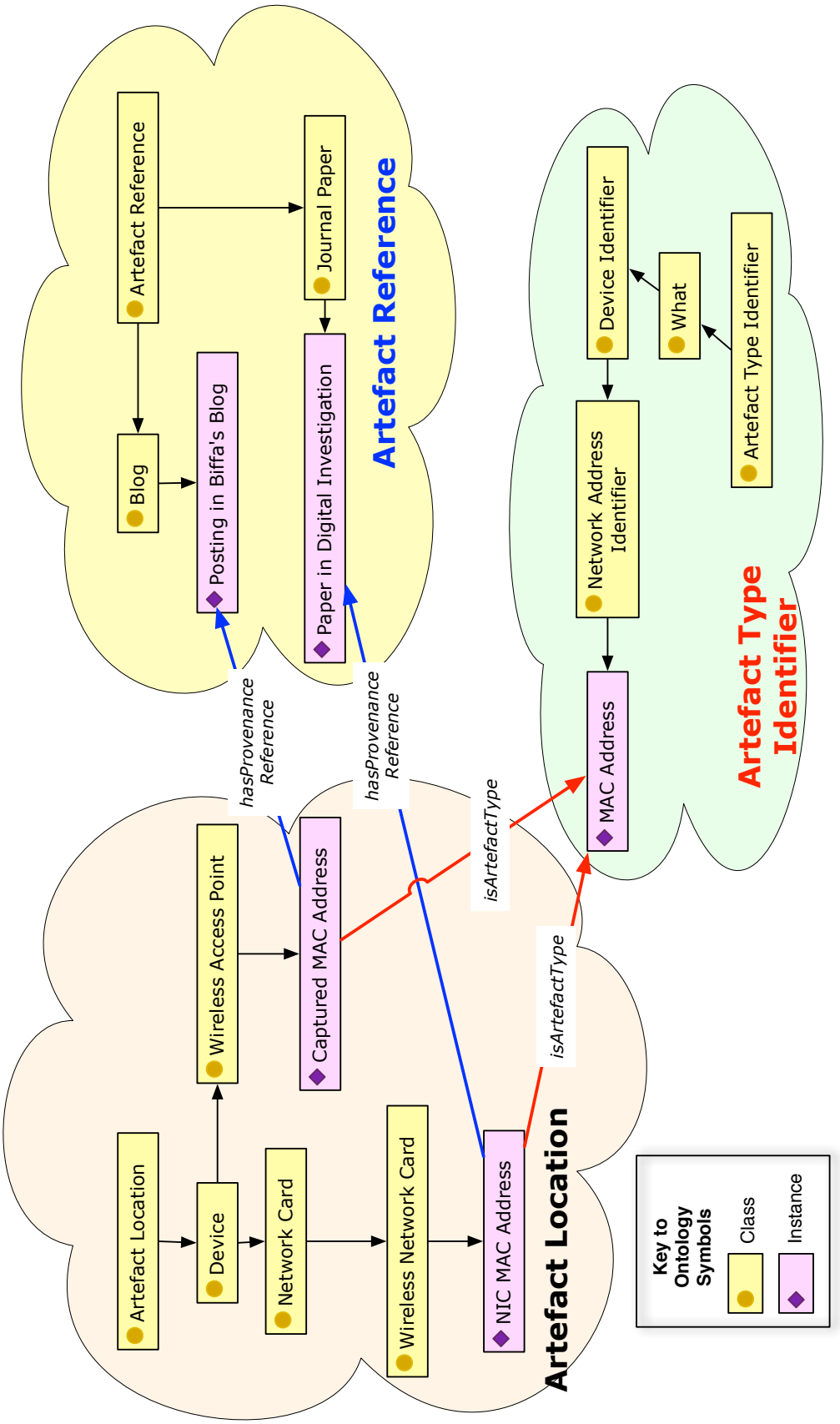

Fig. 4.4 The three DESO classes with two sample artefacts to show population. Note how the "What" sub-class for "Type Identifier" is listed.

Table 4.1

Location - top level class structure

Container	Definition	Comment
Device	Artefacts contained on devices such as serial numbers on USB devices or Media Access Codes on Network Interface Cards	These tend to be hard coded in device firmware and not easily altered. They are present irrelevant of the data stored upon the device.
File System	Artefacts contained within file systems such as Volume Serial Numbers and Volume Label	These are created at the inception of the volume. They can be changed and vary according to the type of file system but are otherwise independent of the installed operating system.
Operating System Independent Application Files	Artefacts contained within files that are not dependent on any other class - such as Operating System. As example, the meta data stored within a PDF or JPEG file.	This is not intended to capture every piece of meta-data in these files - it must be capable of being assigned a Type Identifier.
Operating System	Artefacts contained within operating system files - typically gathered as part of system operation. This could include Volume Serial Numbers in Windows Link files, the serial number gathered when a USB device is inserted or the names of wireless networks to which a device has been connected.	The location and nature of the artefacts will differ dependent on the installed operating system.
Operating System Dependant Application Files	Files generated by the execution of applications within a particular operating system. A contemporary example of this is the messaging application WhatsApp, described by Shortall et al [224], which operates on many platforms but using code specifically designed for that platform - ie platform dependent.	The location and nature of files will vary according to the version of the operating system.

class structure with a comparative lack of value to the investigator in having this complexity specified.

Instead, DESO looks to list only what an examiner requires. To implement this idea, the Location class is simplified with the focus on the class system representing "containers" of artefacts as a structure. Figure 4.5 shows the top level view. These are detailed in Table 4.1.

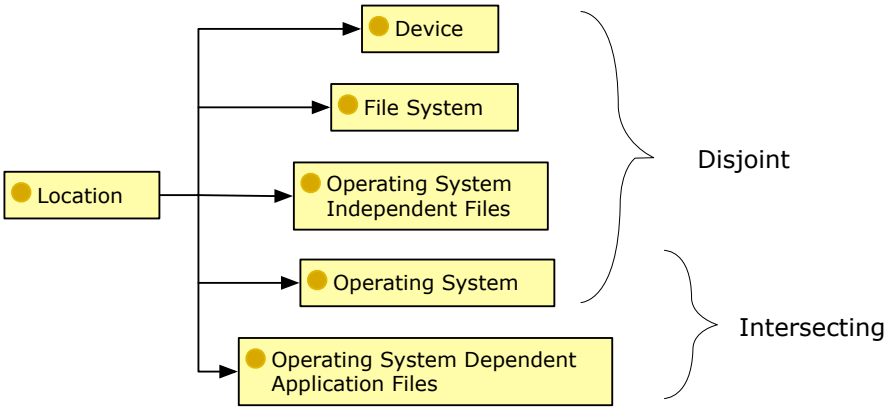

Fig. 4.5 Top-level structure of the Location class

Each "container" within this structure has instances that represent the locations at which artefact data can be extracted by the examiner. The structure only requires sufficient detail to allow the examiner to differentiate one container from another. It does not, for example, require the full path to a file - as will be shown later at Section 4.5.3, this can, instead, be included as a Data Property.

The first four classes are disjoint from each other - so for example, an instance in the "File System" class cannot also be a member of the "Operating System" class. The artefacts found on, for example, a hard disk - such as the serial number in its firmware - are not also found on a file system or operating system. These artefact locations are not connected so the classes are disjoint.

Whilst it is accepted that a device may actually contain a file system and a file system may contain an operating system, this is not the concept being captured by DESO. Each sub-class and descendants is seen as a metaphorical "container" where artefacts could be available. By doing this, the artefacts are normalised so that those found on, for example, a particular File System are identified irrelevant to whether that File System is installed on a USB storage device or a helicopter's satellite navigation system.

The final class, "Operating System Dependent Application Files", has a dependency in that all of its instances must also be a member of at least one of the "Operating System" sub-classes:

$$OperatingSystemDependentApplicationFiles \subseteq OperatingSystem$$

This will be detailed later in Section 4.5.7.

To illustrate the "container" concept, each of the top level containers will be detailed and populated with example instances. In so doing, it will be shown how:

- Instances are named to allow later modification. This will be explained in section 4.5.2 relating to Devices;
- The Location class can be extended and modified to take account of changes in technology and the knowledge of available artefacts. This will also be explained in 4.5.2, Devices; and
- The presence of an instance in a class means that it is available for all its sub-classes. This will be illustrated at Section 4.5.8 when the placement of instances is explained.

These all assist in answering Research Question 2 - adjusting to changes in technology

The Device sub-class will first be detailed and used to introduce some of the key concepts. Next Data Properties will be introduced followed by the other Location sub-classes.

4.5.2 Location sub-class: Device

As the name suggests, the Device sub-class is a structure of containers for the artefacts that can be located on devices. An instance in this class represents such an artefact location. This is illustrated in Figure 4.6. The sub-classes are listed only to a level of detail necessary for an examiner to identify a device and so assess what artefacts are available.

So, for example, current Hard Disks contain at least three items of interest: Manufacturer, Model and Serial Number. All Hard Disks should have this data. As such, it is unnecessary to subdivide this class into, for example, disks containing spinning platters and solid state disks. This further delineation does not change anything in terms of the artefacts that are available.

But for Network Interface Cards it is worth delineating further as there are differences. For example, a wireless Network Interface Card will also have a Service Set Identifier (SSID)

The instances, shown in purple (with diamonds), are the actual artefact locations. Each instance has properties giving further data about this location. These data properties are explained later at Section 4.5.3.

At this stage, two further aspects of DESO will be detailed: the naming of Instances and the extension of classes.

Naming of Instances

If instances are named meaningfully, as shown in Figure 4.6, there is room for confusion. Many of them may have the same - or similar sounding - names. Whilst the instance names could be made longer to delineate them, this is inefficient. It could lead to a situation where instances are given artificially long and obscure names just to differentiate one from the other. Further, a record must be kept of names that have been already used and this must be searched before naming any new instances.

Instead, the "Linked Data Principles"[31] are used - which were previously described in section 2.9.2. All instances are named using a Uniform Resource Identifier (URI).

In DESO, the ontology name is unique, www.semanticweb.org/owenbrady/ontologies/2015/version15# and then either "Artfct", "Type" or "Ref" followed by a sequence number. To illustrate, in Figure 4.6 the entity "SSID" is actually named:

www.semanticweb.org/owenbrady/ontologies/2015/version15#Artfct000009

The name "SSID" is instead included as a "Label" - one of the instance's Data Properties. This has a number of benefits:

- first, it removes any ambiguity - if two researchers call an artefact the same name but they are actually referencing different locations it could cause confusion. Using a URI, the two researchers could create different instances for each of their Locations but their Data Property Labels for the name could be the same;
- second, following on, it allows researchers in different fields to keep names that have a meaning to them. This is useful as it allows reference to a name that they commonly use for communication; and
- third, it helps with extensibility - as will be detailed later in the next section, 4.5.2.

Extension of Classes

A key criterion for DESO's design is that it should be able to extend in order to deal with developments in technology - Research Question 2. To give an example, in Figure 4.6 the class "Hard Disk" contains three instances common to all hard disks. But as research progresses, extra artefacts may be found in Solid State Devices which are not found in other Hard Disks.

This can be captured by the creation of a new sub-class "Solid State Hard Disk" as shown in Figure 4.7. This shows the three original artefacts that can still be found in all Hard Disk types but also one which can only be found in Solid State hard disks.

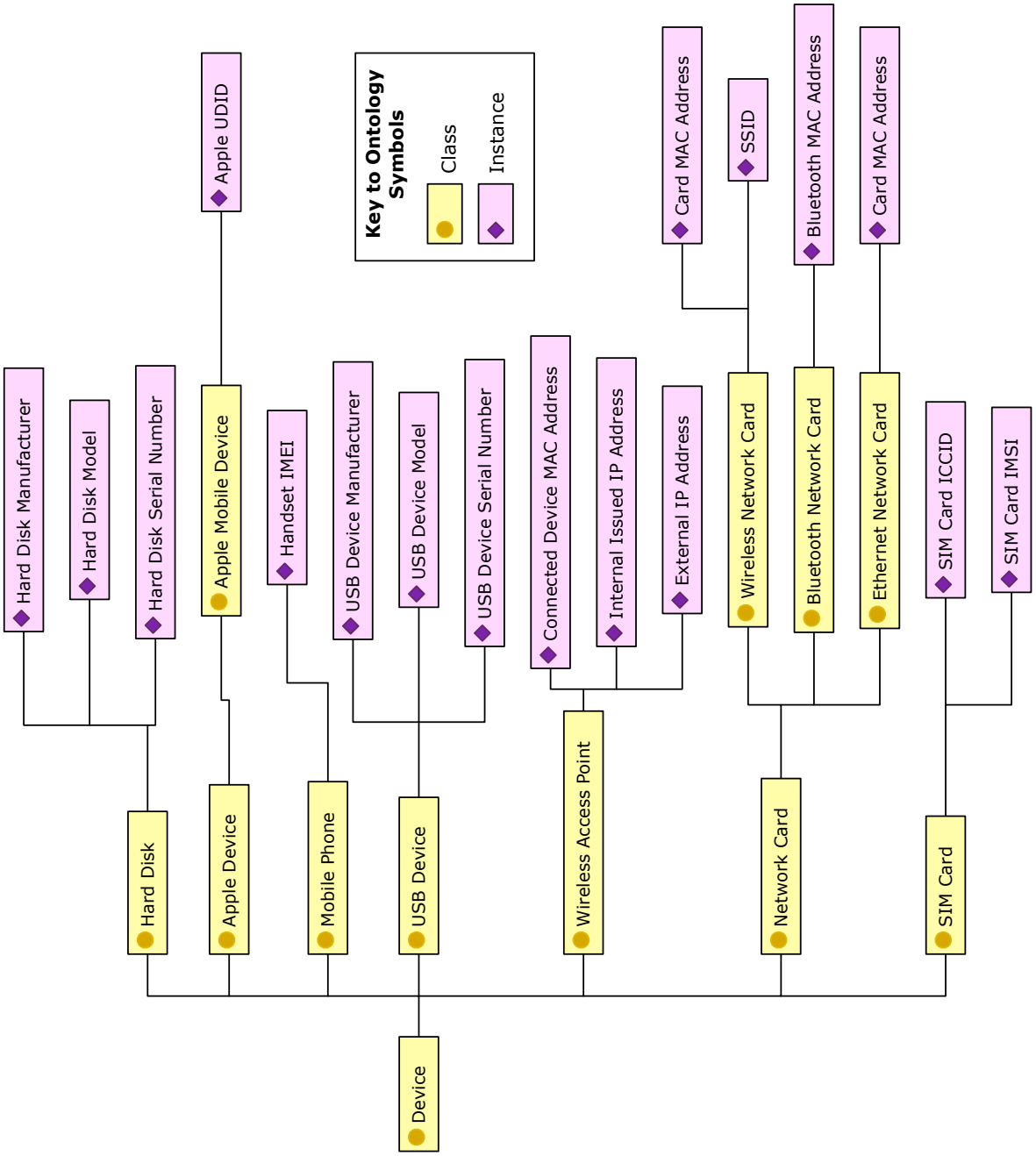

Fig. 4.6 Location Class: Device Subclass. Note that Instance labels rather than URIs are shown for clarity

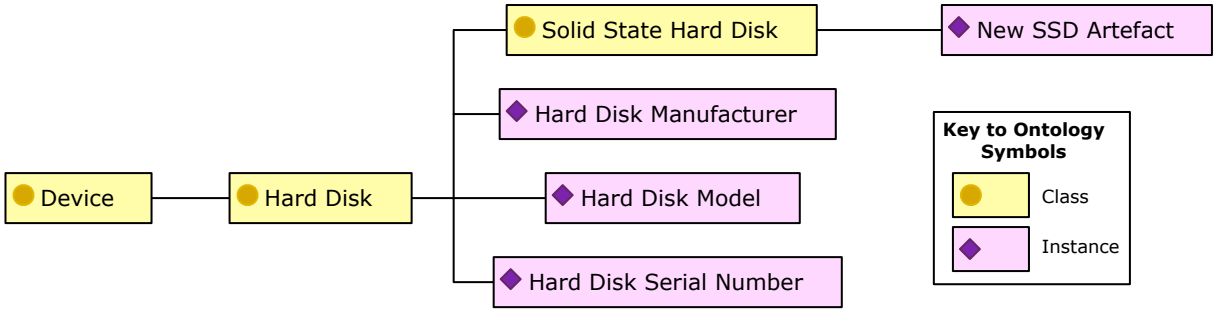

Fig. 4.7 Location Class: the addition of a sub-class for Solid State Devices

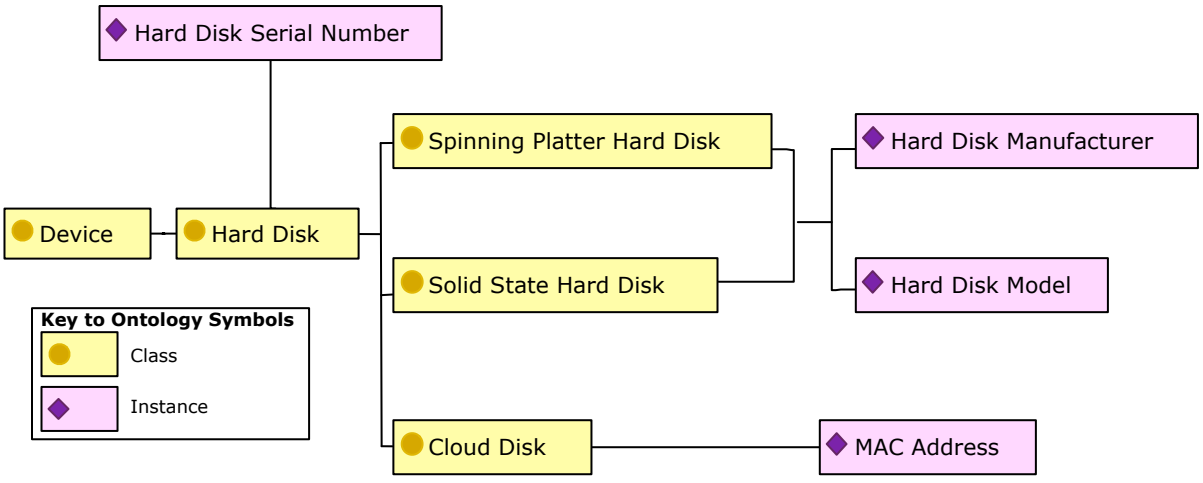

Fig. 4.8 Location Class: the addition of a sub-class for “Cloud Disk” and rearrangement of instances

An alternate scenario is the development of a new type of hard disk, purely for example, called a “Cloud” disk. This no longer identifies itself by Manufacturer and Model but by MAC address. It does, however, still have a serial number. The structure can be adjusted as shown at Figure 4.8. Here, “Serial Number” can still be located in all classes of Hard Disk but this class has been split. The instances Manufacturer and Model are moved into the newly delineated “Spinning Platter Hard Disk” and “Solid State Hard Disks” but they are not contained on “Cloud” disks.

The modification and addition to the class structure is made possible due to the use of URIs - explained at Section 4.5.2. This means the instance names are irrelevant to the class containing them. It allows instances to be freely moved around as the class structures are changed - references to them from other properties will still be valid because they point to the URI itself.

4.5.3 Data Properties

Data properties are the extra information that the user of the ontology needs when assessing an instance. Since the three classes represent different concepts then these properties will vary across them.

For the Location class, typical questions requiring an answer are:

- How can the artefact data be located?
- Can the artefact be refined to a particular user?
- Is the data machine parsable?
- How is the data encoded - e.g. hexadecimal or ascii?

To answer these questions, the data properties for the class are shown at Figures 4.9 and 4.10 but, for context, the full set is also shown at Figure 4.11.

How these data properties answer the posed questions

The location of data will vary according to its container and so the addressing systems must be flexible to take this into account. In some instances, there will be a direct way to obtain the data. In others, there must be a direction to a block of data - such as a file - and then further direction on how to locate the pertinent data within that block. As example:

- devices have artefacts that are typically hard-coded into firmware running a proprietary operating system. Their data may be obtained by issuing a command over the device’s data bus. As example, for hard disks, the ATA specification [9] states the “Identify Device” command can be used to obtain a hard disk serial number; and

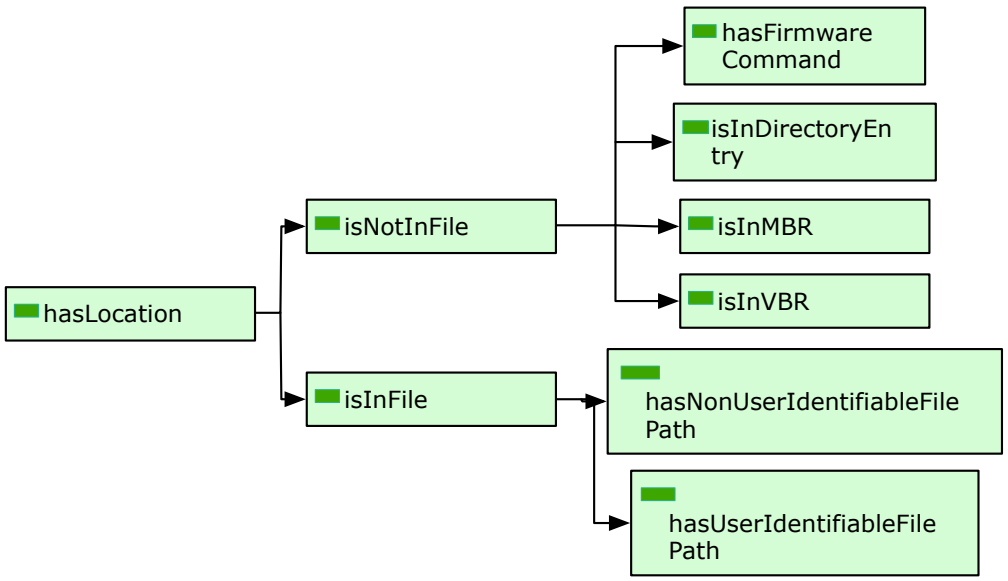

Fig. 4.9 Example Data Properties used in the Location class to show location of a data block

- file systems will have a path to locate the file containing the data. As shown in Figure 4.9 this can be split into those files that are user or non-user identifiable in case the examiner is trying to find artefacts for a single user in a multi-user environment. And once the file has been located, the position of the artefact data within that file must be specified. This is shown at Figure 4.10 with a subset of properties under "hasPosition".

There are still questions concerning data encoding and machine parsability. To answer these the properties shown in Figure 4.11 are used.

The property "hasEntryFormat" supplies information on how the data is encoded. This is important because some conversion may be necessary dependent on the format that will later be required for comparison with other data of the same Type Identifier. For example, the comparison of one FAT 32 Volume Serial Number in decimal with another in hexadecimal will not be effective.

The property "hasParsableStructure' is a boolean value which a forensic tool can interpret: "true" means that there is a set of instructions to allow the data to be extracted. But "false" means the examiner will need to manually interpret the data for this DESO entry.

The question of parsability is one that will be considered further as, despite some solutions being found, this is an area where DESO is still only partially effective.

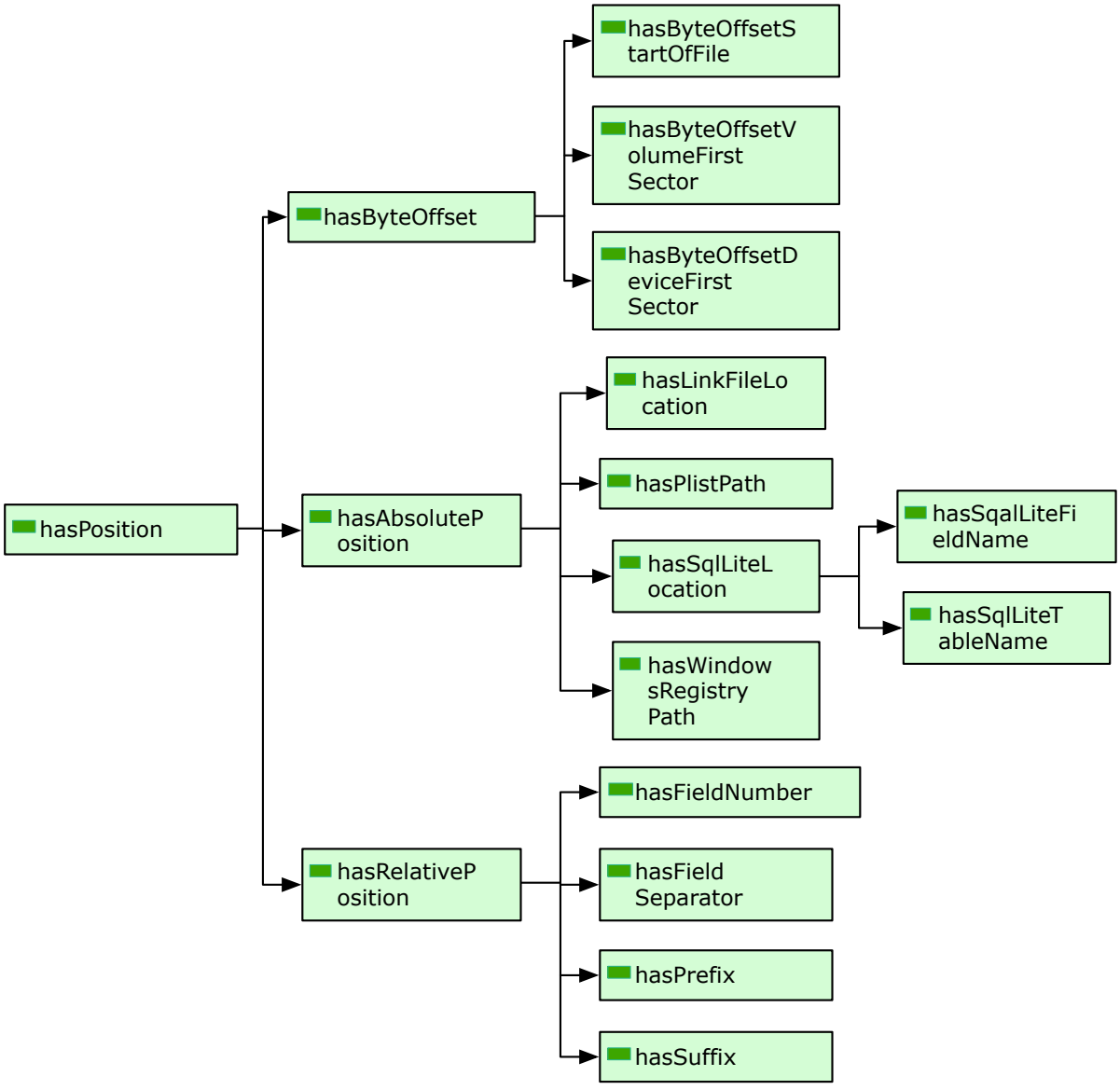

Fig. 4.10 The Data properties used in the Location Class to show position within a block

Some extensible structures could be specified as, effectively, a file path or XML - as demonstrated by Nelson [178]. Examples include the "Plists" found in Apple's OS X or the "Registry" and "Link" files found in Windows operating systems, Solutions were also found for "SQLite" databases by specifying "Table" and "Field" names as shown in Figure 4.11.

But the position of data within a block may be more complex - requiring a number of, interdependent, steps. One approach is to use the Yet Another Markup Language (YAML) [27] as used in the Google Rapid Research Framework (GRR) [58] but this is an area of research that requires further work.

4.5.4 Location sub-class: File System

The File System sub-class is shown at Figure 4.12. Note that, although there are multiple instances with the label "Volume Serial Number" these are not the same. They have different URIs as their location in the respective file systems is different. Also note that "EXT' is not sub-divided into, for example "EXT3" and "EXT4". This is, simply, because at this stage of DESO's development, there are no instances and so further granularity is not required. As shown at Section 4.5.2 the classes can be extended and modified as technology and Digital Evidence research progresses.

4.5.5 Location sub-class: Operating System Independent Files

As the name suggests, this class lists artefact locations in files that exist regardless of the operating system upon which they are contained. A ready example of this is the EXIF data stored in image files such as JPEG and TIFF. Whilst this is commonly known to contain GPS coordinates of where an image was recorded, the standard also has space to record the make, model and serial number of the camera lens used [237, p.68] - a valuable opportunity to link an electronic file back to a physical object. A benefit of DESO is that the potential for this data can be documented and not overlooked.

Because of their independence, it is not possible to use the location of a file as a means of identification. Only the position of artefact data within a file can be specified. This creates a problem in assessing availability and, following on from this, selection to reduce the volume of evidence - Research Question 3.

There is investigative value in these files but caution may need to be used when considering their use. This will be explored later at Chapter 7.

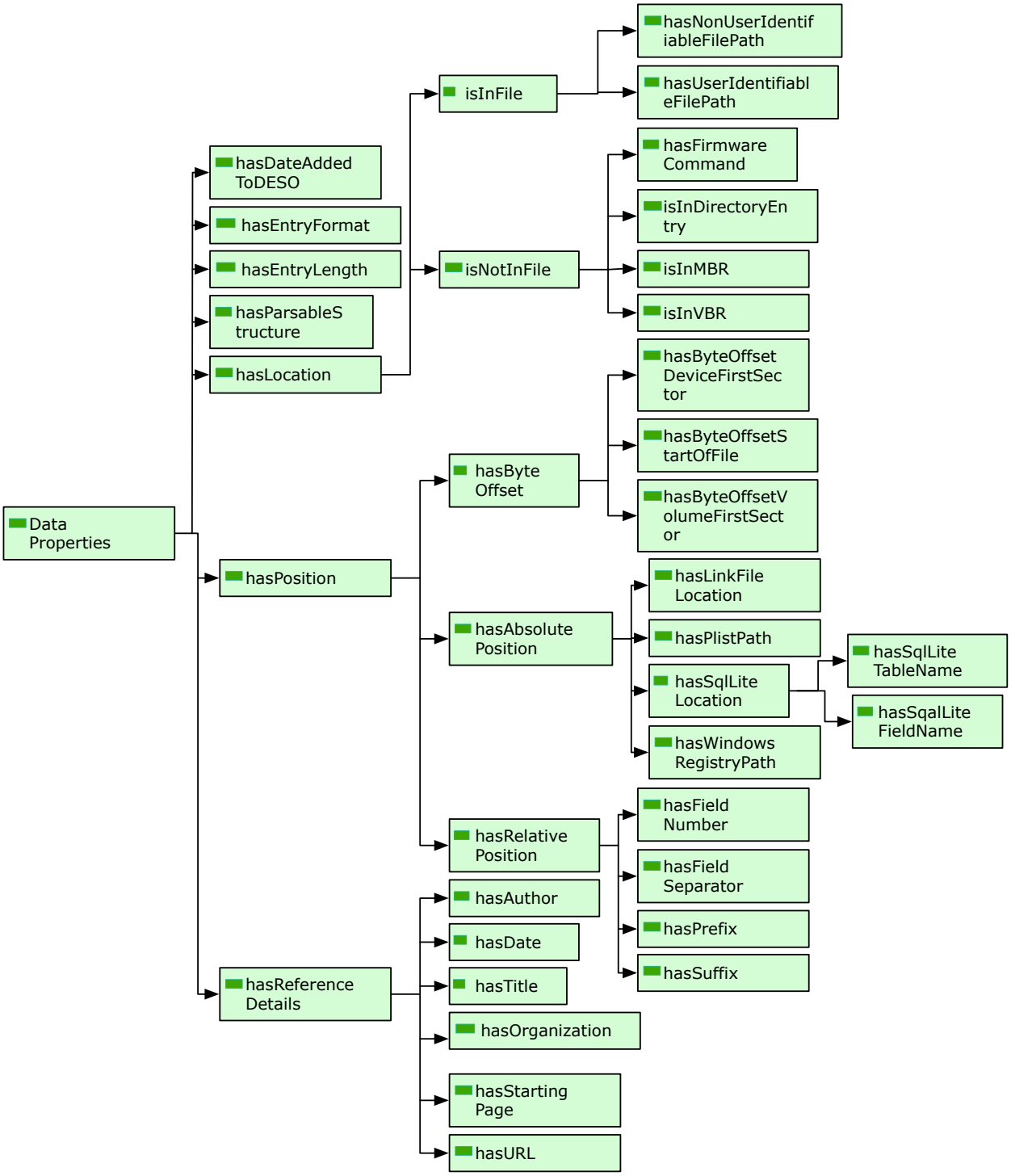

Fig. 4.11 The hierarchy of DESO's data properties

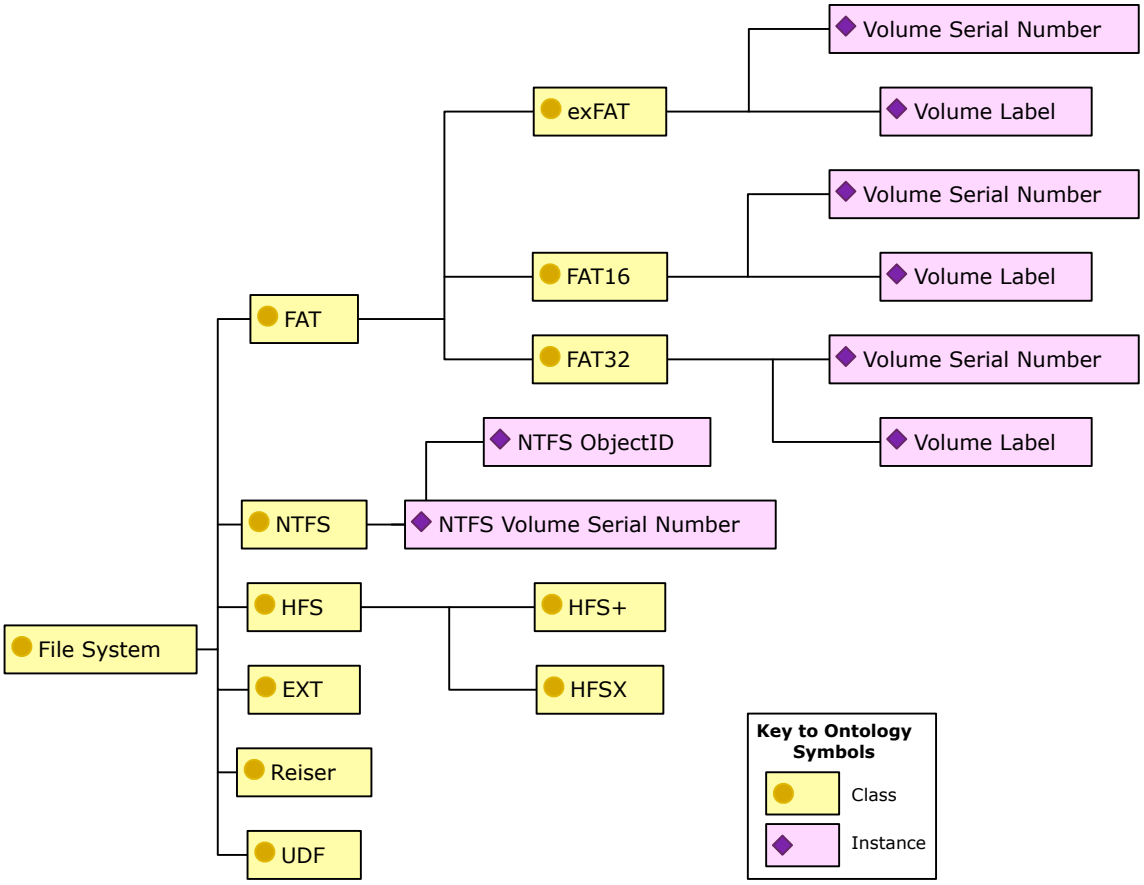

Fig. 4.12 Location Class: File System sub-class. Note that Instance labels rather than URIs are shown for clarity

4.5.6 Location sub-class: Operating System

The Operating System sub-classes again demonstrate the extensibility of DESO. A representative sample is shown at Figure 4.13. As with Devices at Section 4.5.2 the classes are expanded as and when required: “Windows 10” is not expanded as any and all instances are present in all versions of this operating system. But “Windows 7” has been further divided into Service Packs 1 and 2 as there are some instances that are not common to all versions. Representative instances have been shown in Figure 4.13 together with one, “Windows 7 Software Registry EMDMgmt USB Serial Number”, that is common to all versions of this particular operating system.

As new operating systems are developed, they can be added appropriately - for example, an operating system has been developed by Samsung for Internet of Things devices [68]. This can be added under Operating System as a sibling class to Windows and Apple.

4.5.7 Location sub-class: Operating System Dependent Application Files

The reason for considering this sub-class is the increasing use of applications (“apps”) on mobile phones. This was noted by Anglano [12] in his deconstruction of the “Whatsapp” message database on phones running the Android operating system.

The sub-class is different from the others under Location because it is not disjoint from them all. Instead it is dependent on one other sub-class: all instances in Operating System Dependent Application Files must also be a member of an Operating System sub-class.

To explain this step, the Whatsapp application may store its artefacts in a database with a consistent format. The position of artefacts is the same whatever version of operating system the App is running under. But this database file may be located differently according to the operating system upon which the App is installed.

As illustration, Figure 4.14 shows how the application Whatsapp is a sub-class in Operating System Dependent Application Files. It has a GPS artefact contained in the SQLite database that it generates on the device upon which it is installed.

But the location of this SQLite database file will vary according to the operating system - the instances will have differing data properties for this location. As such there are two separate instances - both in the Whatsapp sub-class but also members of respectively different operating systems.

4.5.8 The placement of Instances - what does it represent?

Having explained the Location sub-classes, it is now worth further considering what the sub-classes and respective instances actually represent to the examiner? Figure 4.15 will be used to assist explanation.

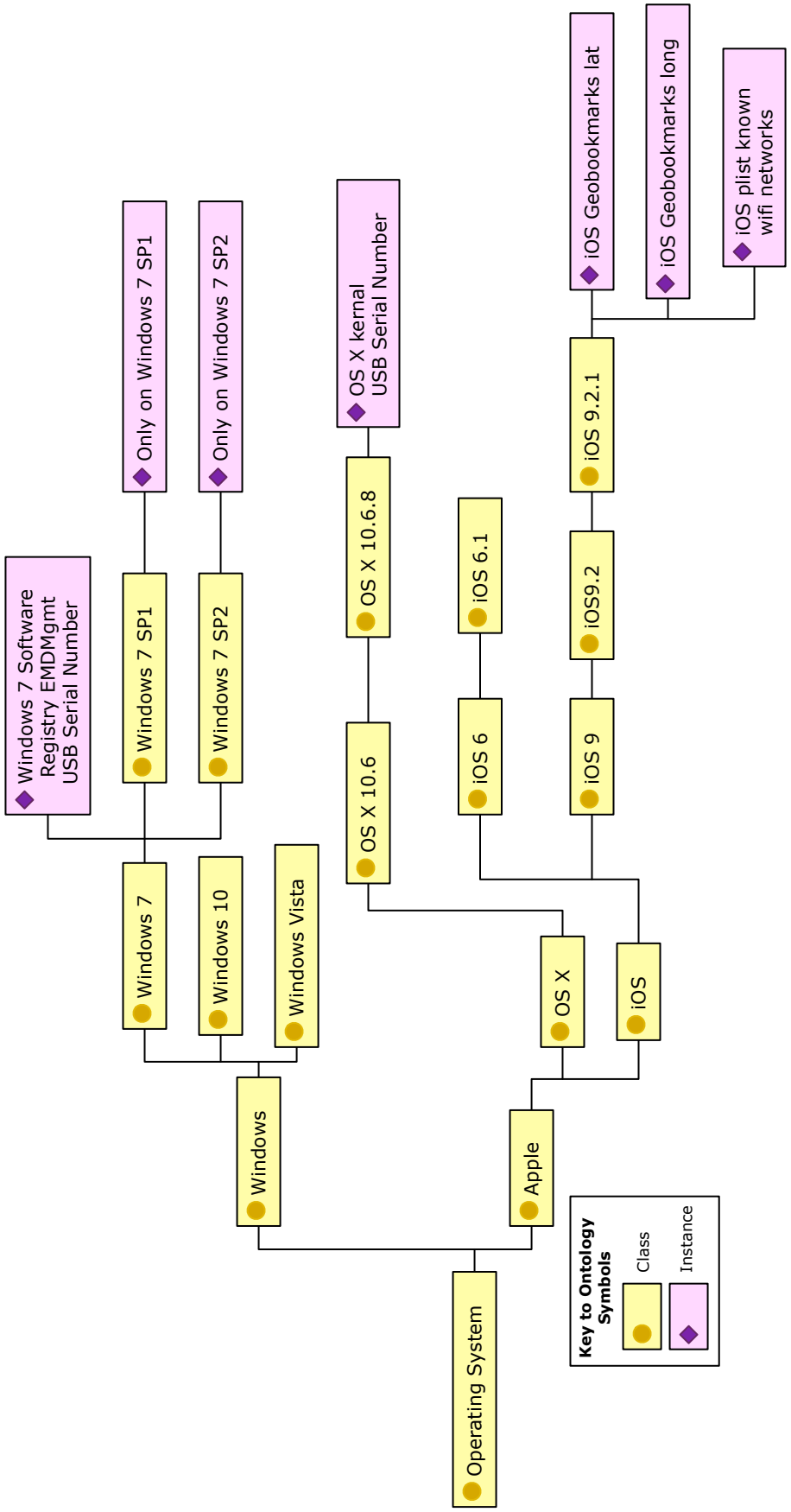

Fig. 4.13 Location Class: Operating System Sub-class. A selection of the Operating System Subclass with example instances

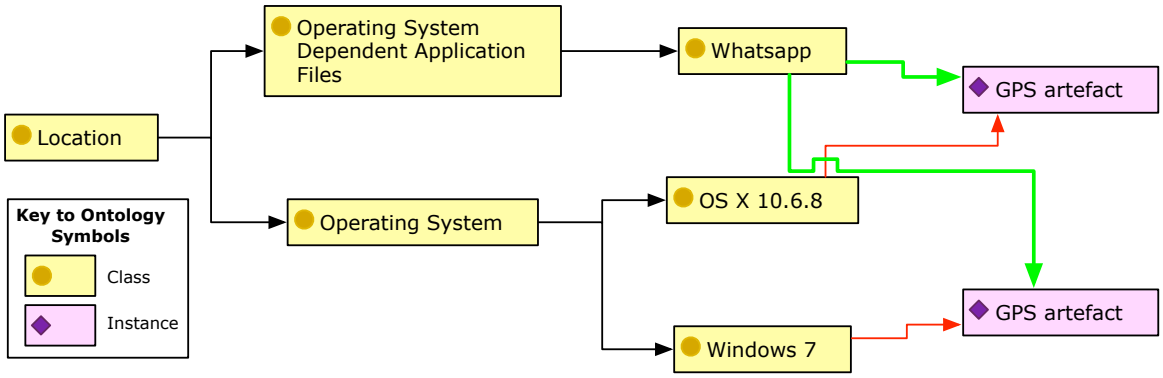

Fig. 4.14 Location sub-class: Operating System Dependent Application files showing two instances produced by the same application but hosted under two different Operating System sub-classes

DESO is set up as a sort-hierarchy in order-sorted logic - as described by Kaneiwa et al [148]. The presence of an instance in a particular sub-class means that a specific artefact is present at the same location for that sub-class and all descendent sub-classes.

So, in Figure 4.15 “Artfct 1” is a an artefact that can be found in the same location on all versions of Windows operating systems. “Artfct 2” can be found on all versions of Windows 7 operating systems but not Windows 10 or Windows Vista. “Artfct 3” can be found at the same location on all versions of Windows 7, Service Pack 1 but not Service Pack 2.

To evaluate the available artefacts, the examiner first assesses which of the top level Location sub-classes, as at Figure 4.5, are present on the item to be examined - eg Device, File System and so on. For each of these sub-classes, the examiner then parses the descendent sub-classes working down through their levels until, either a match is found, or there are no more sub-classes to examine. The conclusion of this process leaves the examiner at the optimal sub-class.

As a worked example, with reference to Figure 4.15, the examiner has found that the item has an Operating System. Further examination has revealed that it is the Windows Operating System. Next, the examiner assesses if there are descendants to this sub-class. There are and so the examiner assesses if the item matches any of these sub-classes - eg Windows 7 or Windows 10. If the examined Operating System matches one, for example Windows 7, the examiner then looks to see if there are sub-classes. Again, there are, and so the process continues.

The process stops when, either there are no more descendant sub-classes, or the Operating System being examined does not match any of them. So, for example, the examiner may reach Windows 7 but is unable to discern if it is Service Pack 1 or 2. In which case, the process would stop at Windows 7.

When this process is complete, the examiner is left at the optimal sub-class and can have confidence that all of the artefacts in that sub-class and its ascendants contain instances that are locations of available artefacts.

This process is complete when the process is reversed and the examiner works back up the sub-classes to the top of the Location Class gathering all these instances.

At conclusion, the examiner has all the available artefacts for a given digital evidence source.

4.5.9 Summary

A class system for Location has been outlined and it has been shown how this structure can be modified and extended to cope, not only with developments in technology but also the continual discovery of digital artefacts. In this way, a repository is created that allows an examiner to understand what artefacts may be available.

But this class system does not assist with selection and correlation since it is capturing all the available artefacts.

Finally, the artefacts have no provenance - if, for example, something is described as a USB Device Serial Number and it is accessed using a certain command, what is the justification for this assertion?

For the answers to these questions, two further Classes are needed: the first is Type Identifier and the second, Reference. The next chapter will explain these concepts.

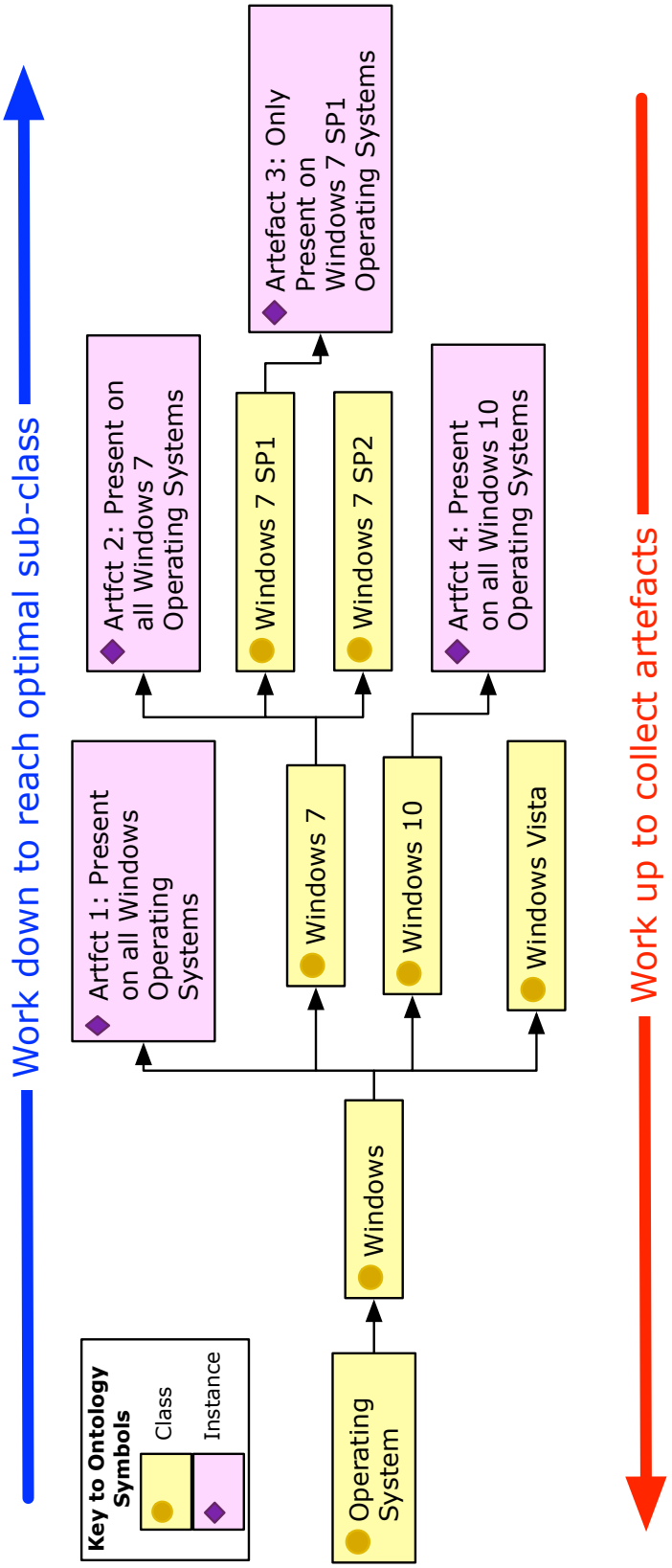

Fig. 4.15 Location sub-class: Illustration of Operating System with contrived instances to illustrate how placement affects the availability of artefacts.

Chapter 5

DESO - Addressing Selection, Correlation and Reliability

The Location class demonstrates that the artefacts available from a particular source can be documented. But this documentation does not assist in assessing which of those artefacts will be of use for an investigation, comparing them and assessing their reliability. The aim of the Type Identifier and Reference classes is to address these problems.

5.1 The Type Identifier class

5.1.1 The Aim of this class

To provide a mechanism for selection and correlation, the available artefacts in the Location class need to be linked to a suitable, definitive, Type Identifier. This represents the meaning of the data and allows only the available artefacts of a particular Type Identifier to be extracted rather than them all. This saves processing time and storage space. Those artefacts with the same Type Identifier can be compared - wherever they are located.

In assessing how the Type Identifier Class should be structured, the primary focus is that all artefacts should be linked to the lines of enquiry in an investigation. As shown at Section 2.1, these are always centred on answering What, Who, When, Where, How and Why (5WH) questions. So it seems logical to group the artefact identifiers under these headings as shown at Figure 5.1. In this way all Type Identifiers will have a relevance to the investigation.

First, it is worth exploring the 5WH categories to understand their meaning in a Digital Evidence context. This is shown at Table 5.1.

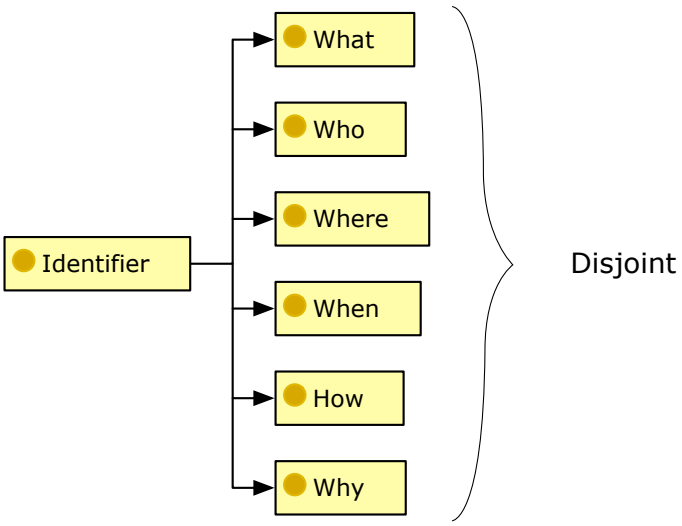

Fig. 5.1 Top level structure of the Identifier sub-class

5.1.2 The 5WH principle

A brief inspection of Table 5.1 shows that representation of some these terms may be more practicable than others. This is due to the degree of interpretation required of the data before it can be assigned a meaning. As examples:

- the definitive GPS coordinates in “Where” - which require no further interpretation;
- a recorded time in “When” - which can be affected by the clock of the machine recording it and the various times zones in use around the World; and
- the more nebulous “How” and “Why” - can there be any single artefact that can answer these questions?

This will now be explored in more detail.

5.1.3 What

As earlier shown in Table 1.1, common forensic science techniques rely on comparison of one piece of data to another. This can be the mark left by a suspect’s finger or their deposited DNA or a tool found in their possession when compared against the various marks and traces left at a crime scene. The “What” category is important because its components provide material for the digital equivalent of this trace evidence - the identifying traces left when one piece of equipment or software interacts with another.

The consideration of issues that should be included in this category are those - and only those - identifiers which would provide some positive benefit to an investigation. The structure of sub-classes is shown at Figure 5.2.

Note that, at the top of the structure, there is a split between “Device” identifiers and “Logical” identifiers. The reason for this division is that Device identifiers are intended to

Table 5.1

Exploring the application of 5WH to Digital Evidence

Term	Definition [91]	Application to Digital Evidence
What	Information specifying the nature or identity of something.	Data identifying a piece of equipment or software - such as a serial number
Who	What or which person or people?	Data associated with a person - such as a name or user name. This could also include an organisation
When	At what time?	Data identifying when a specific event took place - such as the interaction of one piece of equipment with another
Where	In or at what place?	Data connected with a geographic location - such as the GPS coordinates that can be embedded into an image file when it is created.
How	In what way or manner? By what means?	Data that defines the process before an event took place - such as how a device was being used before a telephone call was being made.
Why	For what reason or purpose?	Data that defines a motive before an event took place such as internet searches before visiting a particular location.

be such data as the serial numbers embedded in firmware. Examples are the MAC address in a Network Interface Card (NIC) or a mobile phone handset IMEI. Logical Identifiers are those which are recorded by software and more easily changed - such as a file system Volume Label.

Whilst there are reports of Device Identifiers being modified [97] or spoofed [263] this change relies on a deliberate act in contrast to the Logical Identifiers which are likely to change as a system is in normal use. As such, there may be a case for choosing the Device Type Identifier category first - when there is a choice - as they are less prone to change.

In defining sub-classes and instances, the focus has not been on the different types of technologies but, instead, the identifiers they could contain. These identifiers translate data into information that could be used in an investigation.

In following through this principal, when evaluating potential "Location" artefacts, if data - in the form of a device, file etc, cannot be linked to a recognised Type Identifier, it should not be included. This is because the data is of no use to the investigation. All Location entries must be linked to a Type Identifier entry.

The instances contained in the Type Identifier class are linked from instances in the Location Class by an object property: "isArtefactType".

The naming of instances using URIs was previously covered at Section 4.5.2 and also applies to this category.

Data properties

For type Identifiers, the data properties are less complex than Location. There is no need to specify how data might be found - only how it should be displayed. This is important to ensure that data from disparate sources is comparable. As such the only properties are "entryFormat" and "entryLength".

Extensibility

As discussed at Section 4.5.2 it is important that the Location class structure is able to modify and expand as technology and research progress. The same principles apply for Type Identifier as they do for Location: as new technologies are introduced and researched, they can be added as a sub-class under Device or Logical identifier. If an extra Type Identifier is found, it can be added as an instance under the appropriate sub-class.

Whilst the class structure is presently quite simple, this may change as DESO develops. Because URIs are used, the sub-classes and instances can be rearranged with no impact on other instances referenced to or from them. This is because the reference is to the URI and not the class structure or name.

5.1.4 Who

Introduction to Friend of a Friend

As explored at Table 5.1, the "Who" category aims to identify data associated with a person or organisation. This could be, for example, a name, a user name or correspondent.

Whilst no existing classification was found for the "What" category, a long standing candidate does exist for "Who": Friend Of A Friend (FOAF) - " a computer language defining a dictionary of people-related terms that can be used in structured data" [39].

FOAF has become recognised for articulating this type of data. Its use has been examined in early studies: 2005, [158], and 2008 [114]. But there is less contemporary

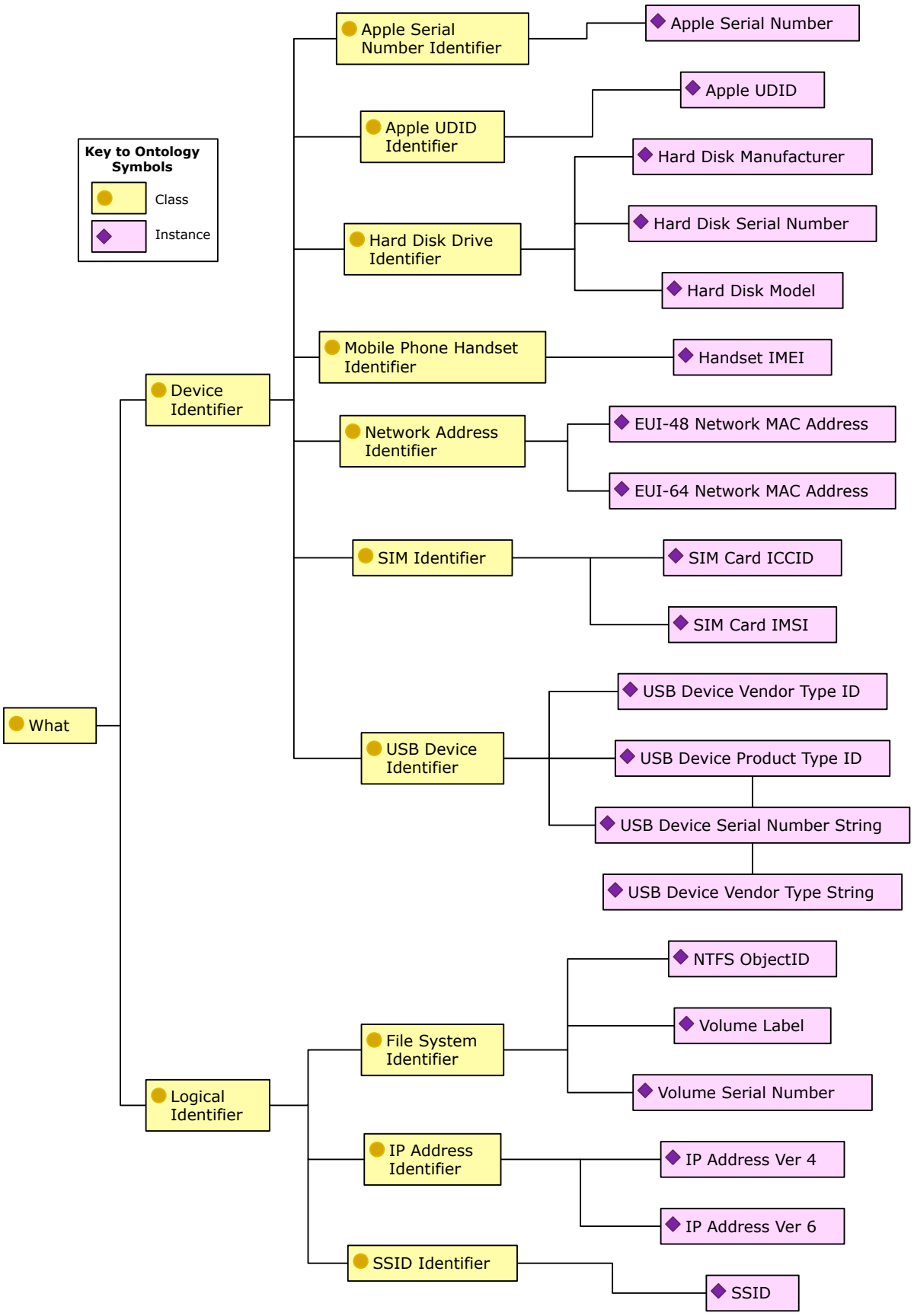

Fig. 5.2 Identifier Class: the What sub-class. A sample of instances are shown for illustration. Note that, again, labels are displayed instead of URIs for ease of reading.

evidence of its wide-spread employment - only the anecdotal Linked Open Vocabulary survey [37] by one of FOAF's original developers. Nevertheless, as previously noted in section 3.2.5 there are advantages in making use of other ontologies.

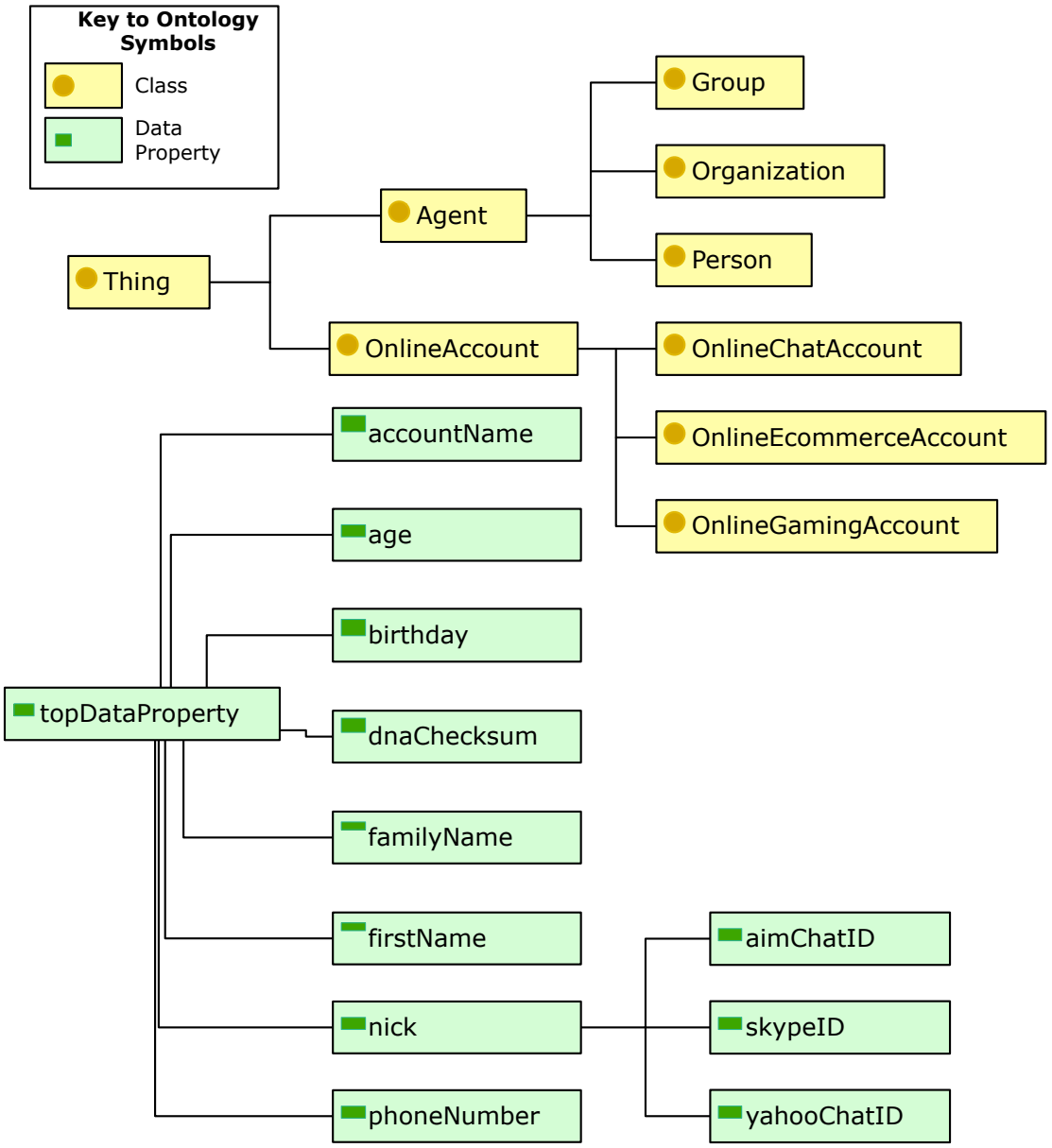

Fig. 5.3 A section of the Friend of a Friend Class structure (coloured yellow) and data properties (coloured green) from the "Paddington" version [38]. Note the limited options for online account identifiers in the data properties.

As shown at Figure 5.3, FOAF has a simple Class structure. The data properties are of interest because they could become the instances used in DESO for the Who Type Identifiers.

The version of FOAF used in DESO was published in 2014. But despite its currency, it can be seen that the selection of data properties is limited - not including many of the common social media applications - such as "Snapchat", "Twitter" or "Whatsapp" - in use

at the time that this thesis is being written. Indeed, the noted transience and short life of these applications [143] will pose problems when contrasted against the considered and time-consuming development life-cycle of specifications such as FOAF.

Application of FOAF to DESO

In considering whether FOAF is suitable, consideration must first be given to DESO's requirements. In essence, these are minimal - purely the ability to assign a Type Identifier to artefacts concerned with persons, organisations or user names.

But consideration should also be given to the granularity of this identification. For example, if the details of a Facebook [96] account are stored in a Windows operating system Registry, is it enough to assign it a type Identifier such as a "FOAF:accountName" as shown in Figure 5.3 or does it have to be particularised to Facebook - for example "FOAF:accountNameFacebook"?

The answer is not certain so it is prudent to cater for more detailed requirements. The solution is to use FOAF classes to delineate the types of artefacts that will be identified and use FOAF data properties as instances to form the type Identifiers. But new instances can be created as required.

This is illustrated at Figure 5.4. The displayed classes are from FOAF and so are the instances for the "Person" and "Organization" sub-classes - as can be referenced in Figure 5.3. The instances for the 'Online Account" sub-class have been added as they do not occur in FOAF.

The referencing to FOAF is useful because it allows any extracted data to be readily compared to other Linked Open Data that has been typified using these same terms. Further, FOAF specifies a format for the various data. This makes it more likely that data will be matched. But the new Type Identifiers, such as "Twitter ID" could still be identified if the examiner searched for all instances in the the "Online Account" sub-class.

5.1.5 Where

In describing the "Where" category a number of points are covered:

- the reuse of existing ontologies, as discussed at section 3.2.5, is continued;
- the concept of multiple instances for the same artefact data is introduced; and
- it is shown how DESO could alert an examiner to available evidence which had not been previously considered.

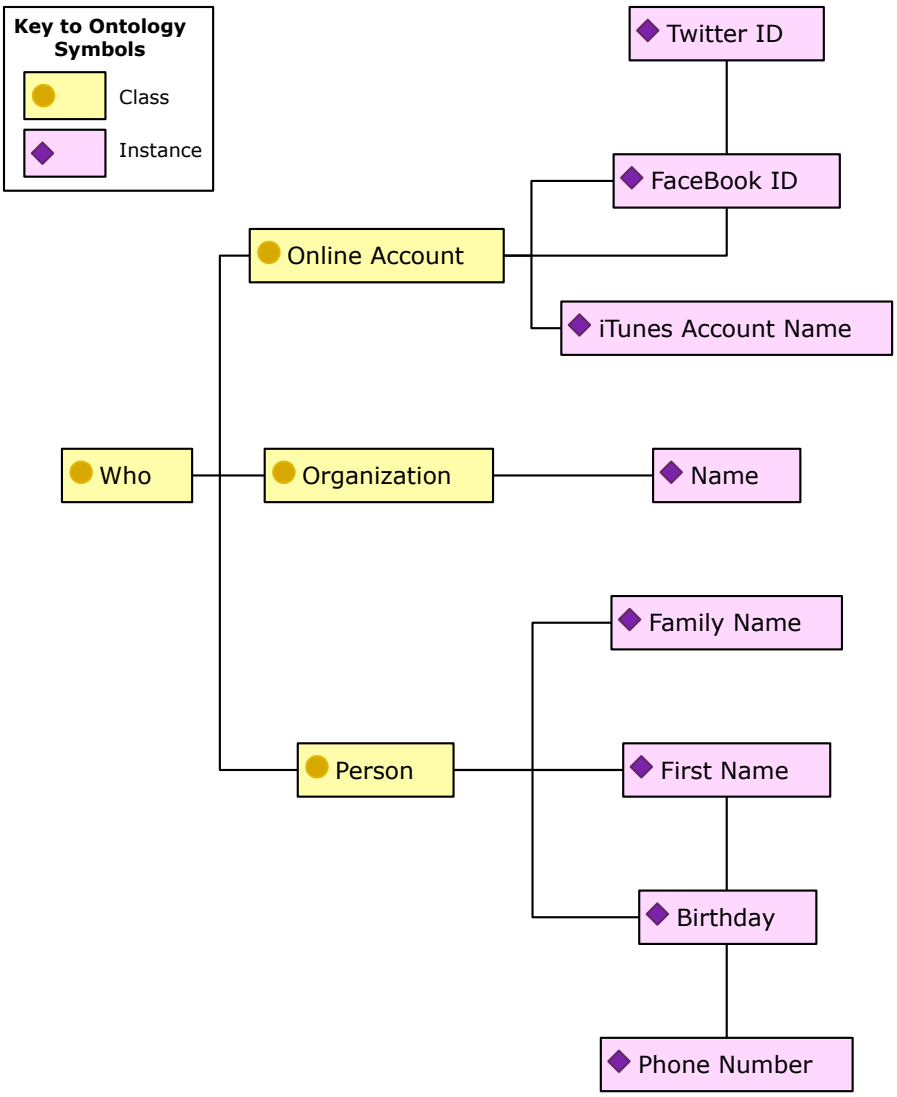

Fig. 5.4 Identifier Class: the Who sub-class. All classes are from Friend Of A Friend (FOAF). All instances with the exception of those in "Online Account" also from FOAF.

The structure of the Where category

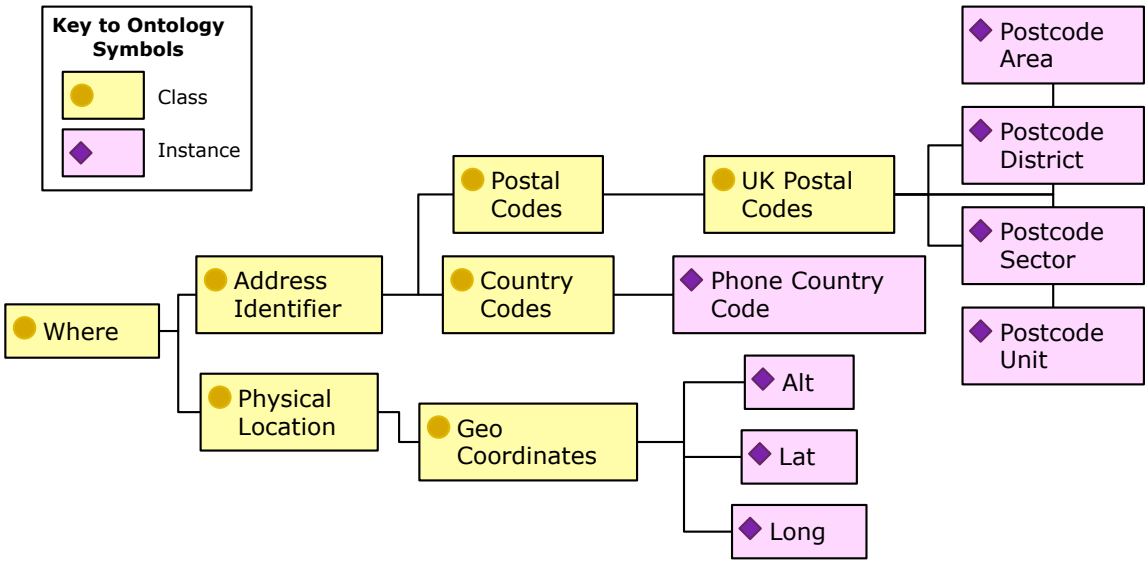

Fig. 5.5 Identifier Class: the Where sub-class

In the same way that a distinction was made between Device and Logical identifiers for the "What" category at Section 5.2, the concept has been carried through to "Where". Instances in the "Address Identifier" sub-class are naming concepts that could change over time in contrast to "Physical Location" where change is less likely. In specifying the instances a number of existing ontologies / standards have been used. These are:

- The Postcode ontology [183] produced by the UK-based Ordnance Survey
- The RDF vocabulary for WGS84 latitude/longitude/altitude markup [253] produced by W3C
- The The International Public Telecommunication Numbering Plan [142] produced by the International Telecommunications Union

In so doing, DESO identifiers will link in to other sources of data used by investigators.

Same data - multiple instances

The concept being discussed in this section is how the same data can have different meanings to an investigation - and how DESO copes with this situation.

Figure 5.6 illustrates a SIM card which contains an ICCID. This is a nineteen digit serial number with a defined format [120, pg7]. The first two digits, "89" reference that this SIM card is for telecommunications purposes. But the second two or three digits are a country code: in Figure 5.6 this is "852" for Hong Kong.

So this data actually contains two pieces of data of interest to the investigator:

1. the whole ICCID is a serial number which can be matched to a serial number elsewhere - with a “What” type identifier; and

2. a section of the ICCID is a county code indicating the country in which the SIM is to be used - with a “Where” type identifier.

The question is whether this data should be represented as one Location instance with an Object property to two different Type identifiers or two Location instances which each point to their own Type identifier?

There are hazards with the former solution: first, the locations aren’t exactly the same. The ICCID is the whole nineteen digits but the country code is just two or three of them. Second, the reference source justifying the link to the Type identifier may not be the same for both pieces of data.

As such, if a single instance is being created in the Location Class which has multiple Type Identifiers there must be careful checks. This is to ensure that, first, the data properties for the Location instance remain the same no matter which of the Type Identifiers is used. And second, the Reference Class entry is also the same for these Type Identifiers. Otherwise, multiple instances should be created in the Location class.

Display of hidden evidential uses

With further consideration of Figure 5.6 it can be seen how the Type identifier can alert an examiner to uses of evidence that may not have been considered.

Suppose an investigation concerns the discovery of a corpse pulled from the sea - the first task is to identify this body. If a SIM card is found on the corpse then DESO can be queried for the evidence that may be contained on it.

Both the ICCID in the “What” category and the ICCID Country Code in the “Where” category will be highlighted - so alerting the examiner that this person may have a connection to a particular country and providing a useful line of enquiry. Unless the examiner was regularly examining telecommunications data, this is an aspect that might be overlooked.

This illustrates the importance of concentrating on the semantic representation of the data rather than the technical one.

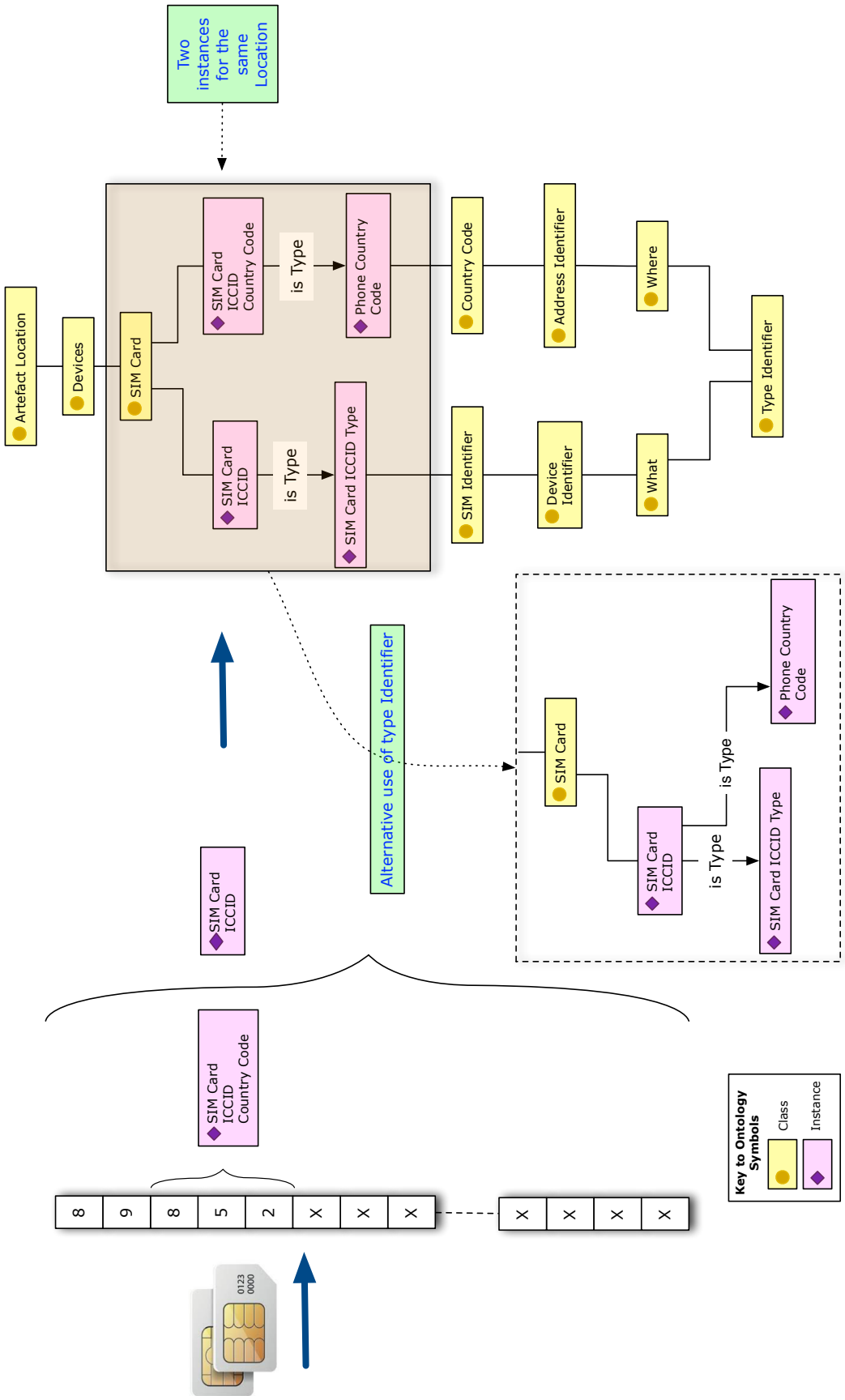

Fig. 5.6 An Illustration of how one section of data - SIM ICCID illustrated - can be multiple Locations and Types

5.1.6 When

Defining Type Identifiers relating to time is more problematic than for the preceding 5WH categories due to the ubiquity of timestamps in a modern digital device. Willassen [259] cites a number of examples:

- File systems have multiple time stamps per file - indeed each file contained within NTFS has at least eight [36, p.228].
- Systems usually record events from their processes in logs. Each event has a timestamp.
- Network equipment such as http, pop, imap and dhcp servers typically log each user transaction in a system log. Each transaction may have a timestamp.
- For email, the SMTP protocol mandates each server to add its identity and a timestamp to a transmitted email. Email messages therefore contain many timestamps.
- Messaging protocols, such as SMS in GSM, also add server generated timestamps to each transmitted message.
- Many mainstream applications such as word processors, spreadsheets and web browsers generate timestamps and store them as part of their specific file format.

If DESO merely listed the locations of these time stamps without assigning any meaning to them then this would not assist with the problem of selection. How would an examiner assess which of these were required - Research Questions 3 and 4.

But there could be problems when assigning a Type Identifier due to the degree of interpretation required for the data [65] [32]. This falls into two areas: technical and semantic.

Technical interpretation of time stamps

There are a number of issues that can impact on the correct interpretation of a time stamp:

- The acccuracy of any clock used will have a direct effect on the accuracy on any time stamp using that clock;
- The resolution of the time stamp - for example, in FAT file systems, the “Last Accessed” time stamp is only a date with no time [259, p.8]. This leaves a large window for an event to have taken place; and
- The time zone setting on a computer may have an impact on the interpretation of the data. This is demonstrated by NTFS time stamps - which are stored with respect to Universal Coordinated Time (UTC) [36, p.259]. If a Windows computer has its time zone set incorrectly and then it is later corrected, the file time stamps set before the correction will be inaccurate when displayed to the user after the correction.

Semantic interpretation of time stamps

At section 2.9.5, the use of time-lines was discussed and, also, their drawbacks. The semantic interpretation of time stamps is a key factor in these limitations. Figure 5.7 illustrates this problem.

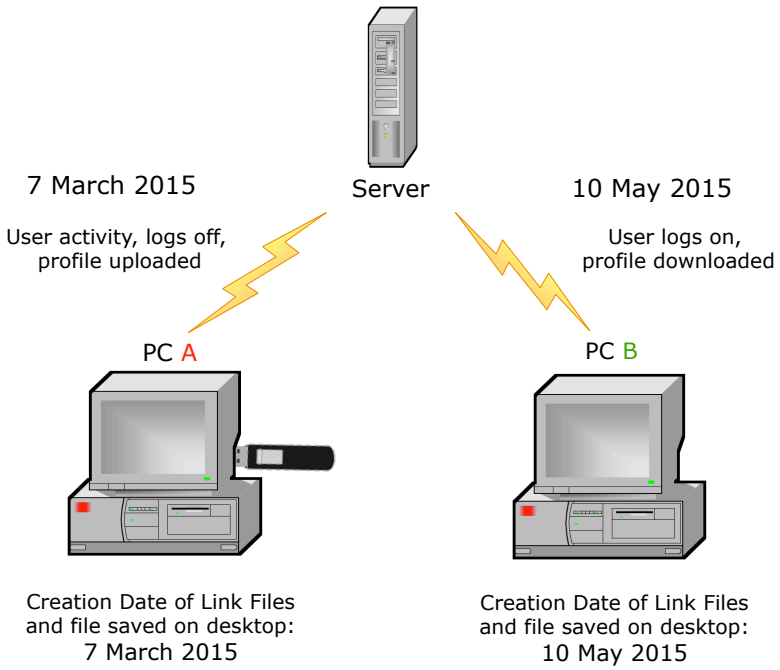

Fig. 5.7 Illustrating the problems of time stamp interpretation using roaming profiles - what does the Creation date represent?

If a user logs on to PC "A" where roaming profiles are enabled and then accesses a file on a memory stick, a Link file is created. If this is the first time that a file of this name has been accessed, the creation date of this Link file is the time of this access [194].

When the user logs out of the PC, the profile is uploaded to a central server. When the user later logs on to PC "B", the link file is downloaded to the PC. But the Creation time stamp is not that of the access to the file but of when the user logged on to PC B and the Link file was downloaded as part of the roaming profile.

So in summary, the same file appears on two different computers but the Creation date represents two different concepts: one is the time that a file with a particular name was accessed, the other is the time that a user logged on to a particular computer.

And delineating between these - and other - concepts is only possible by reference to other data sources. It is hazardous to make assumptions based just on one source of data [32].

How to represent When?

A viable solution for a Type Identifier has to avoid the highlighted problems of technical and semantic interpretation. Instead it has to focus on considering what time stamps

an investigator would want to know and then supplying as many reliable artefacts as practicable.

In this respect, considering a time stamp on its own may be meaningless - it is just a time. The utility of time stamps is when they are the meta-data for an event.

As previously discussed at section 2.9.5, there has been previous work on the representation of a time by Hobbs [134] and Pan et al [191] leading to the W3C working draft "Time Ontology in OWL" [74]. But these do not offer assistance on the meaning of time from an investigative context. Indeed Pan et al assume that "another ontology provides for the description of events, either a general ontology of event structure abstractly conceived, or specific, domain-dependent ontologies for specific domains" [134]. DESO has to provide this assistance.

The approach in DESO is to use the When category to act as meta-data for the type Identifiers in the What, Where and Who categories. For example:

- *When* did a person go to a location?
- *When* was the device connected to a particular wireless access point?
- *When* did a user add a person's contact details to a device?

Figure 5.8 illustrates the sub-classes.

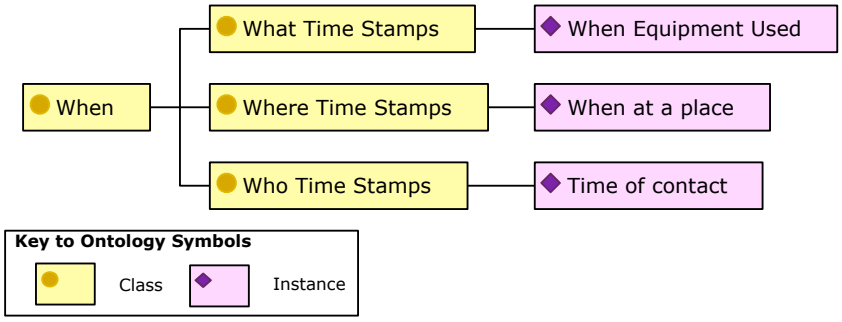

Fig. 5.8 Type Identifier: the When category

To illustrate this further, the process from artefact to DESO record will be followed step by step.

Figure 5.9 shows an extract from a presentation on iOS artefacts [89]. These artefacts document when a device encounters a WiFi hotspot. A file "cache_encryptedB.db" can be parsed and records selected from a database table named "WifiLocation".

Instances can be recorded in the iOS 9.0.2 Location sub-class to represent these artefacts.

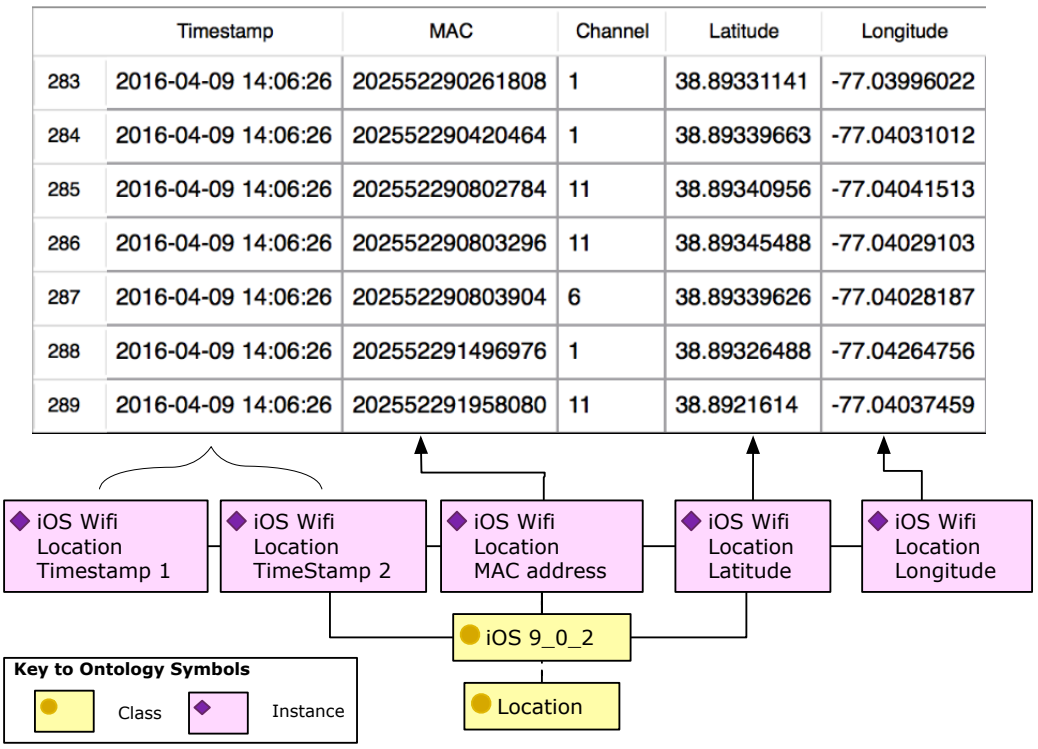

Fig. 5.9 The use of the When Type identifier Stage 1: Extract from presentation on iOS artefacts by Edwards [89] with relevant artefact locations shown. Note there are two instances for the time stamp.

When assigning suitable Type Identifiers, note that there are What records - the MAC address - and Where records - the displayed GPS coordinates “Latitude” and “Longitude”. But the time stamps for these records are semantically different. For the MAC address it is the time that this equipment was encountered. For the GPS coordinates, it is the time that the device was in this location.

It is important to make these distinctions because of how DESO will later be used by investigators. If a geographic Type Identifier is used, then a question such as “Where was the device being used on 15 January 2017?” can be answered by reference to geographic identifiers in the “Where” sub-class. Conversely, an investigator may ask a question such as “Was this device used in the Peckham Internet Cafe on 15 January 2017?” With knowledge of the internet cafe’s WiFi network name, this question can be answered by reference to an SSID type entry in the “What” category.

Figure 5.10 shows how these Type Identifiers are assigned. Note, it is important that a time stamp is not recorded in DESO unless the precise meaning of the data is understood - otherwise the hazards outlined in the section 2.9.5 regarding time-lining are not overcome.

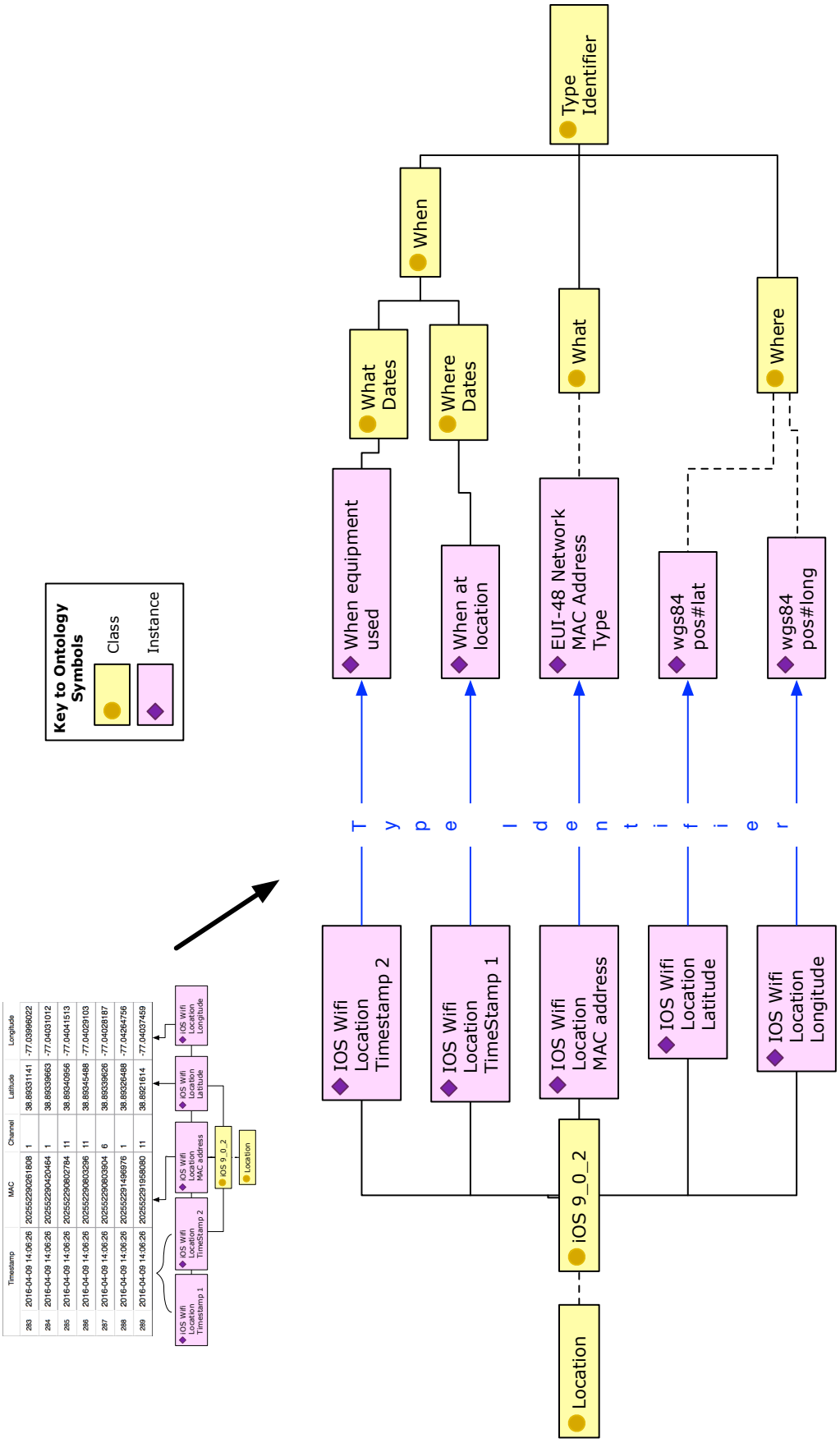

Fig. 5.10 The use of the When Type identifier Stage 2: The artefact Locations displayed in Figure 5.9 are assigned a Type Identifier. Note that "Timestamp 1" and "Timestamp 2" have different identifiers - from, respectively, the "What Dates and 'Where Dates" sub-classes.

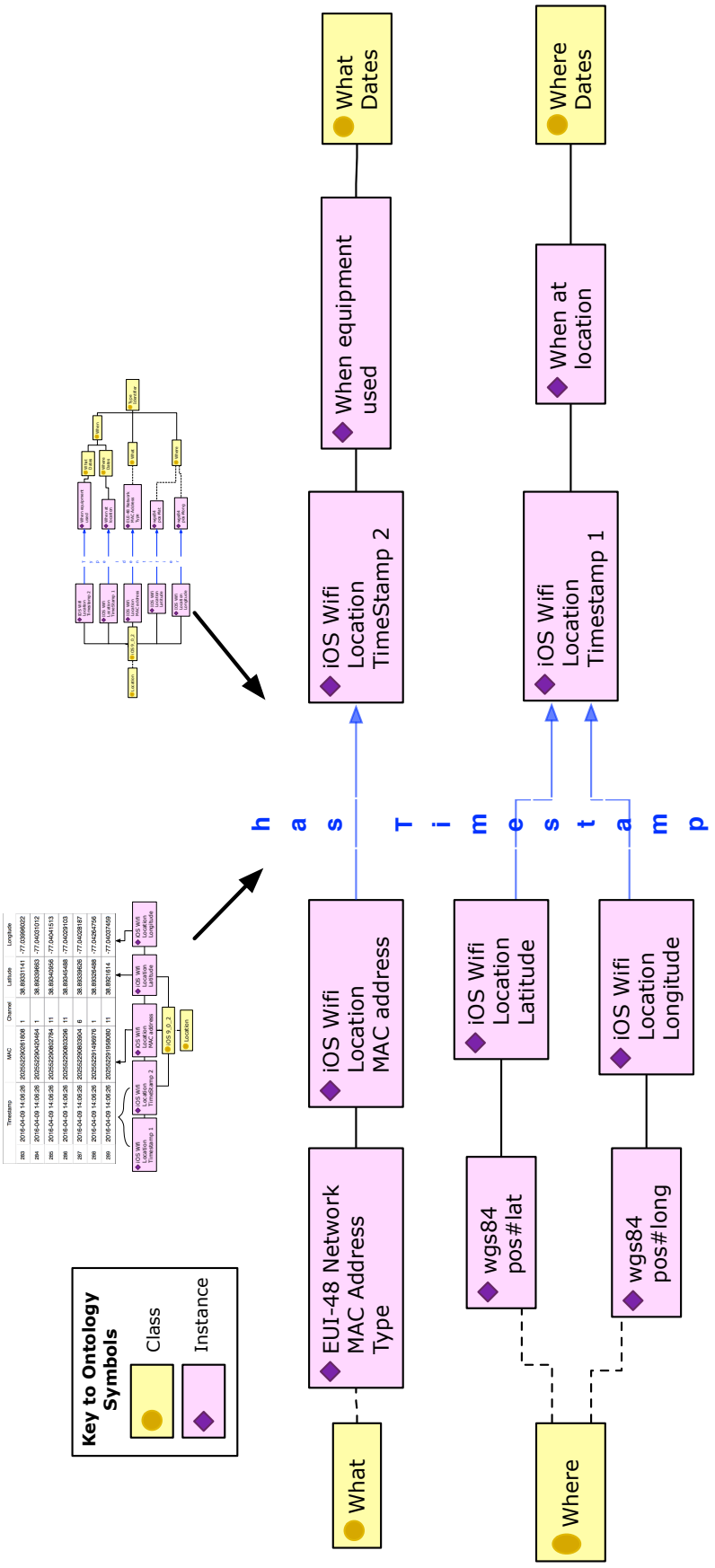

Fig. 5.11 The use of the When Type identifier Stage 3: a new Object Property, "hasTimestamp" is used to link the What or Where Location to the time stamp location. The When Type Identifiers are used to convey what this time stamp represents.

Figure 5.11 shows how the When Type Identifiers are brought into use by means of a new Object Property ”hasTimestamp”. This is from the artefacts with What, Who and Where Type Identifiers to those with a When Type Identifier. Again, for clarity, the time stamp is seen as subservient to the other artefacts and the process for recording should be:

1. Identify Location and type Identifier of What, Who or Where artefact
2. Identify if there is any associated time stamp
3. Assess whether there is clarity on the meaning of this time stamp - can it be assigned a Type Identifier from the When sub-class? If so record and link with the “hasTimestamp” Object Property.

5.1.7 How and Why

The classes of “How” and “Why” are more complex than the others. As discussed at Section 5.1.2:

- “How” can mean in what way or manner or by what means and includes data that defines the process before an event took place - such as how a device was being used before a telephone call was being made.
- “Why” describes the reason or purpose for something and includes data that, for example, defines a motive before an event took place. An example would be internet searches before visiting a particular place.

These are compound queries not easily satisfied by one particular artefact but, more likely, a combination of them leading to a conclusion for an action or series of events. This chimes with the Level 3 provenance described earlier at Table 2.1 - which described the inferences that could be drawn from any given artefact - what does it actually “mean”?

This topic will be discussed further when DESO is evaluated at Section 7.3

5.2 The Reference class

In order to assess the reliability of any artefact and its Type Identifier, it is important to know the basis behind this assertion. The technological world develops rapidly so, given the time delay caused by the process, it would be unrealistic to expect all artefacts to have appeared in a peer-reviewed journal. As already documented, there is a wealth of useful information on available artefacts being published by researchers using transient media with no formal peer review process - such as web blogs.

DESO aims not only to include this information but also to capture the nature of the source. In this way an examiner can decide whether further research or experimentation is required - particularly if the recovered artefact data is of importance to a case.

To allow for the representation of provenance, DESO has a system for documenting the source and weight of the information behind the artefact and its Type Identifier. As introduced in section 4.4.2, the third and final class is artefact "Reference". This is how an examiner can understand the reason why data at a particular location means a particular thing.

There are two aspects to answering this question: the first is recording the source of the information for the assertion; and the second is documenting the type of provenance this information provides - is it just a pronouncement on a blog or a detailed laboratory study with test data and results for others to replicate?

These two aspects will be covered in turn.

5.2.1 Recording of reference source information

The Bibliographic Ontology [79] (BIBO) was chosen to record the reference sources due to its wide use - a section of BIBO is shown at Figure 5.12. Other ontologies such as the FRBR-aligned Bibliographic Ontology (FaBiO) and Citation Typing Ontology (CiTO) were reviewed [195] but found to be more complex than required in terms of concepts and classes.

Only a section of BIBO's classes are required but one extra, "Developer Pages" was added - as shown in the example at Figure 5.13. This is to distinguish that these pages contain technical data from an authoritative source. As covered previously, due to the use of URIs when identifying the instances in DESO, new sub-classes and structures can be added and the instances rearranged.

5.2.2 Expression of provenance type

An examiner may not want to be restricted on a choice of artefacts when making an initial assessment of evidential sources. Mention of useful data locations from such sources as internet blogs may be of great utility. But once useful data is found, then consideration needs to given to the source of any information about artefact locations and their meaning. Otherwise, there is the risk of misleading an investigation or - worse - a court.

Each individual in the artefact Location class has an object property from the *hasProvenanceReference* set. This is a hierarchy of properties which describe the information source used to assert that the observed data is a particular artefact Type Identifier. The classification is an adaptation of the Evidence and Conclusion Ontology [112] which was developed for the Gene Ontology [16] and is shown at Figure 5.14

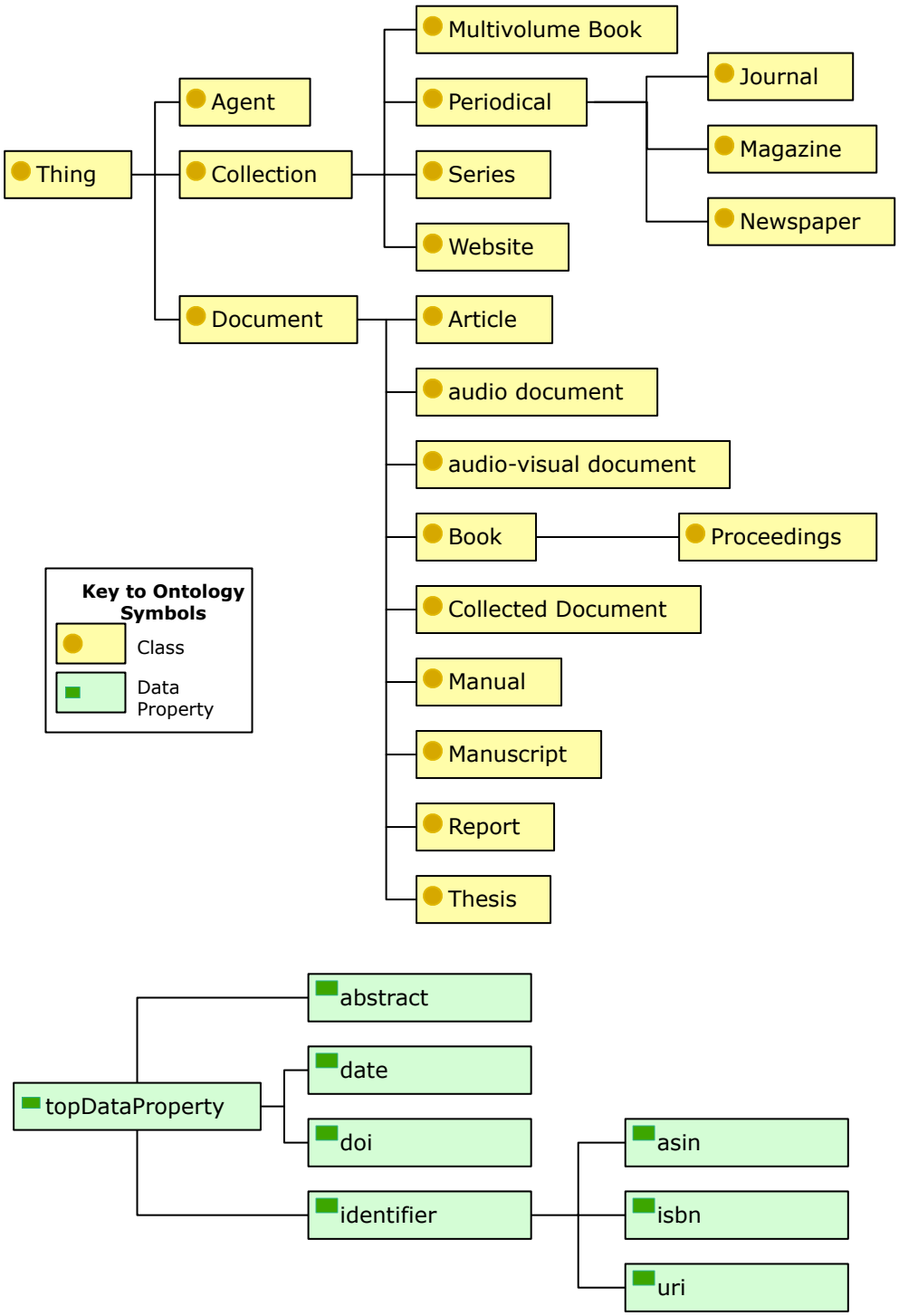

Fig. 5.12 A selection of the Bibliographic Ontology version 1.3 [79] classes and data properties

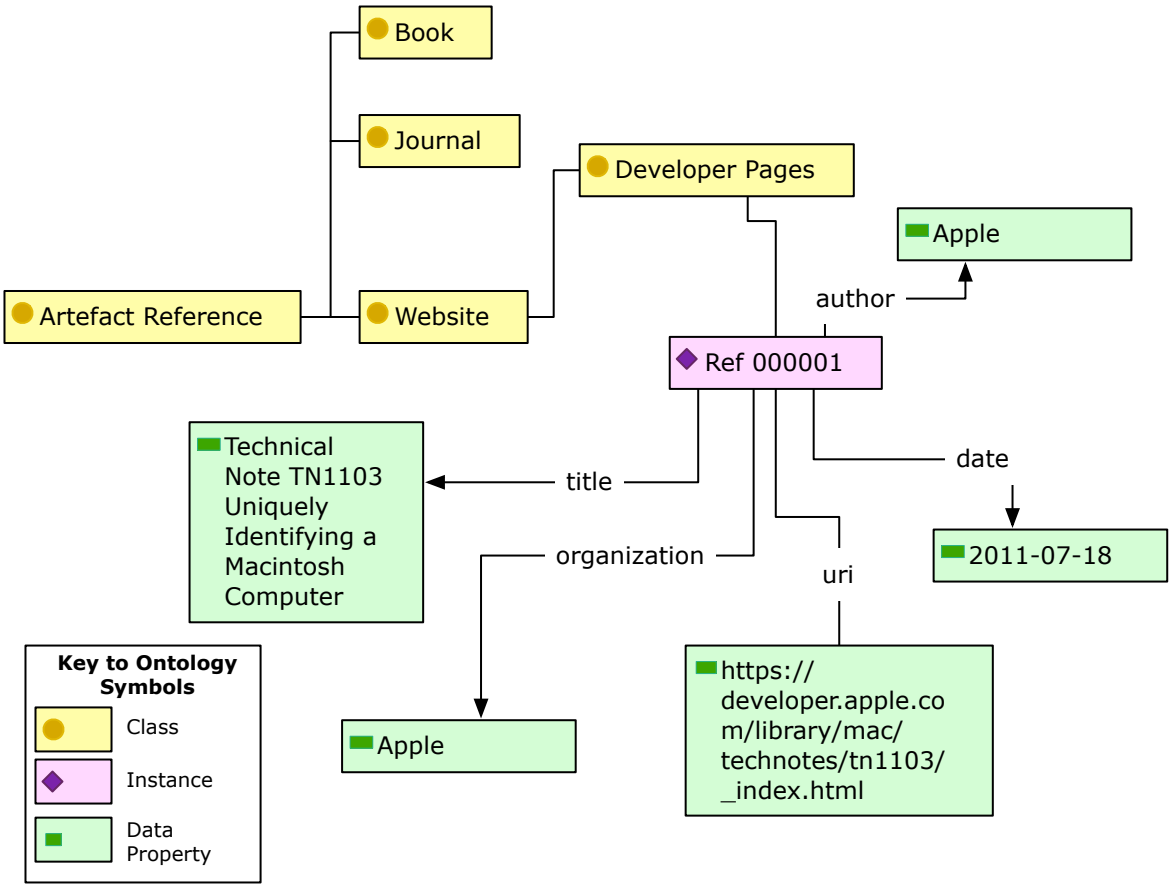

Fig. 5.13 The Reference class structure. Note the sub-class “Developer Pages” has been added. Also shown is a sample instance, “Ref 000001” with related data properties.

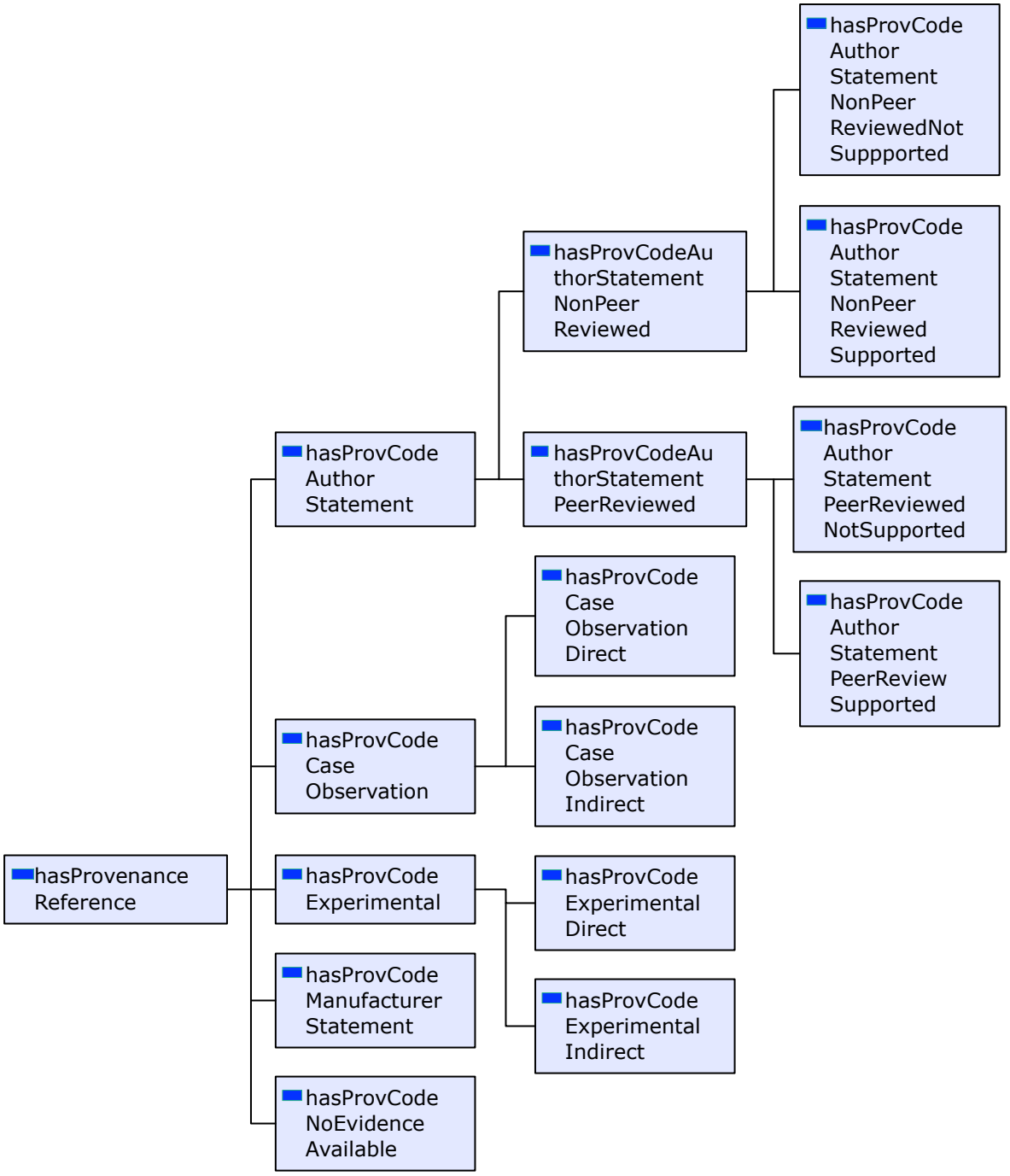

Fig. 5.14 The set of object properties between the Location and Reference classes.

The hierarchy has the following tiers:

- Author Statement - an assertion made in a published text of some nature - for example this could be in a book or journal or on a blog. This hierarchy is further divided to distinguish between author statements that are peer reviewed and also whether there are supporting details of experimentation or availability of data used for testing.
- Manufacturer Statement - technical specification on the function of system by a manufacturer or standards body such as Apple, Microsoft, USB Association or IEEE.
- Observation - the artefact has been observed by the examiner on previous cases either of the same or similar type of data.
- Experimentation - the examiner has conducted testing to understand how the artefact data is created.
- No Evidence Available - There is no evidence to support the assertion that the represented data is the artefact type.

5.3 Summary of DESO

This chapter has introduced DESO. In so doing it has shown how:

- the locations of useful evidential artefacts can be recorded in a class structure. This structure can be modified and extended to cater for new technology - such as the Internet of Things - and the discovery of new artefacts;
- the identified artefact Locations are assigned a Type Identifier which allows the comparison of data from diverse sources in a consistent format. The identifiers are arranged in a class structure matching investigative questions; and
- each artefact Location / Type Identifier pair are linked to a reference source to show where this assertion originated and an object property describes the nature of this reference in relation to the assertion.

The next chapter will examine an investigative scenario. This is used to test how monolithic tools would be used to approach a particular investigative question and how DESO can be used to overcome any identified shortcomings.

Chapter 6

Comparative test application and evaluation of DESO

6.1 Introduction

Chapters 4 and 5 introduced DESO. This chapter details its application. Following this, Chapter 7 critically evaluates the effectiveness of DESO's application to understand if it successfully addresses the research problems and where further work is required.

The scenario chosen for testing DESO is its assistance when using monolithic tools. The reason for this choice is the widespread use of these tools. It follows that, if DESO is to provide assistance, its impact would be greatest in this area.

The generation of test data was detailed earlier, in Section 4.2.2. This same data will be used again as follows: The method employed when testing DESO was as follows:

- A hypothetical investigation scenario involving the test data was devised;
- A selection of monolithic tools was assembled;
- The tools were first applied to this data to understand how they could assist; and
- DESO was then applied to the various tasks to understand if the effectiveness of the monolithic tools could be improved.

6.2 Investigation scenario

The scenario to be considered is that a suspicious death has occurred in a house containing two computers. A person was seen running away from the premises and a suspect matching this person's description was arrested some distance away. When searched, he was found in possession of a USB memory stick.

When interviewed, the arrested person denied ever having visited the dead person's house and he is now detained pending enquiries.

There are non-digital enquiries that need to be performed which include assessing if this person has left any physical traces at the scene - such as fingerprints or DNA.

But the job of the digital evidence examiner is to quickly discover if there is anything regarding the USB memory stick that will link the suspect to the scene.

6.3 Selection of monolithic tools

Three tools were assessed:

- Magnet Forensics Axiom - Examine and Process v1.0.5.1994 [162];
- Encase Version 7 [123]; and
- Belkasoft Evidence Center Version 8.4 [26].

The selection of tools was based solely on availability of software. Findings were common to all three tools but Axiom is principally described - purely as an exemplar, not because it performed better or worse than the other two. The findings should be viewed as suggestions for improving the use of these tools - not as a reason for discontinuing their use. This point is referenced again in the findings at Section 6.9.

6.4 Consideration of tool use

The test scenario is a relatively simple problem: are there any links between the USB memory stick and the two computers found on the premises. The question to be asked when considering the use of monolithic tools is: how should they be used? Where does an examiner begin?

A prudent approach may include an assessment of how any connections between the USB stick and the deceased's computers could be formed. The examiner would then have to discover how artefacts evidencing these connections could be identified, extract the data and then examine them to understand if there are any matches.

The effectiveness of this approach is subject to the examiner's latent knowledge of the artefacts and reference sources documenting others that are previously unknown. The examiner would also require skill in using any tool to ensure that data for the the identified artefacts is correctly extracted from any source.

Alternatively, the monolithic tools may have some sort of module or process that would automatically perform these tasks - and then it would be for the examiner to assess the tool's effectiveness. But the problem with this approach has been detailed at Section 2.11.2: the tools are not explicit when stating the artefacts they can and cannot extract. So how can an examiner have confidence that all possibly available artefacts have been considered?

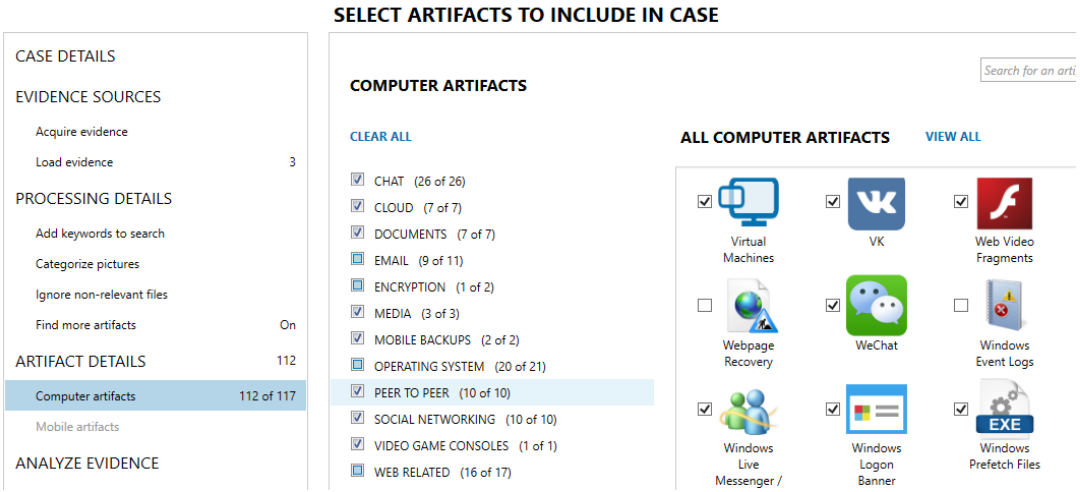

Fig. 6.1 The selection of artefacts to be extracted. Note how the presented artefacts are representative of those categories that Axiom can extract, not those that are available on the item to be examined. This was presented for an OS X operating system

6.5 Test - availability of artefacts

6.5.1 The approach of monolithic tools

Axiom specifies its ability to handle “Operating System” artefacts for Windows-based and iOS systems. What became clear is that the version being tested does not handle OS X operating system artefacts. This demonstrates the difficulty for an examiner in understanding the availability of artefacts on a particular Digital Evidence source based solely on one monolithic tool.

The lack of support for OS X operating system artefacts places importance on the ability to correlate any output from Axiom with tools that do handle this operating system..

Axiom’s data extraction module “Axiom Process” version 1.0.5.1994 was tested. It allows the user to “Select artifacts to include in a case” but this is a generic screen which only delineates between “mobile” and “computer” artefacts. All options are displayed whether or not the actual device being examined actually may contain any of these artefacts.

As example, when the test OS X image was loaded, it offered the option to extract Windows Prefetch files - illustrated at 6.1. But this data did not contain a Windows operating system.

Instead of informing the examiner of the artefacts that may be present on the loaded device, the interface is instead displaying Axiom’s capabilities. This means that the user

may select superfluous processes on data that are not present. Further, the categories are relatively high-level - they do not actually state which artefacts are extracted by these modules and which are not. As a consequence the examiner may miss available artefacts because Axiom does not have the capability to process them.

In summary, the use of a single monolithic tool to assess availability is only effective if that tool displays all artefacts currently known to the field - irrespective of whether or not the tool can extract them.

6.5.2 Improving assessment of availability using DESO

DESO moves any assessment of available artefacts away from the tools used by examiners. As described at section 4.5.8, instead, the examiner uses DESO to work through the functional categories from “Device” to “Application” gathering together a set of artefacts that could be present on the item being examined. These artefacts are listed by their unique DESO number. Tools are then selected on the basis of their ability to extract these DESO artefacts.

To facilitate DESO, the way in which tools document their capabilities will have to change. Instead of the rather generic categoric descriptions now presented to examiners, they will instead have to specifically list the DESO artefacts they can extract.

But there are considerable benefits to this change:

- The examiner has an overall view on available artefacts - not just those presented by any discrete tool. The tools, including open-source ones, can be mixed and matched dependent on requirement;
- DESO provides a ready reference source for tool developers when they are looking to add new capabilities;
- Tool developers can use DESO artefacts with test data to readily verify any changes to tools; and
- The non-tool specific listing of artefacts means that any person wishing to check any findings produced by an examiner can do so without the need to have any tool.

It is accepted that the effectiveness of DESO relies on its population.

6.6 Test - selection of artefacts

Previously, in section 6.2, the described test scenario involved a suspicious death and a fleeing suspect. The task was to check whether there was any connection between the USB memory stick and the two computers found at the deceased’s house.

One approach is to conduct a full examination of all the artefacts present on the three devices and then consider any apparent connections - but this is not time efficient and, most certainly, does not scale well as the amount of devices increases.

Instead, a more strategic approach may be more effective. Discounting physical traces on the devices - such as finger prints or DNA, there are at least two avenues for investigation:

- there may be file content on the USB stick which matches files found on the computer; and
- system records on the computers may indicate that the USB device was inserted and, possibly, accessed. There may also be an indication of when these events happened.

Both are viable lines of enquiry but the second is likely to have more chance of success for the following reasons:

- The first approach may not provide opportunities to link the suspect to the scene unless the content of the files on the USB memory stick gives rise to some form of identification - such as a contract or agreement between the deceased and the suspect; but
- the second approach could be the quickest line of enquiry because it may highlight individualising data - such as a serial number linking the USB memory stick to the computers.

This second line of enquiry will now be considered.

6.6.1 The approach of monolithic tools

With regard to assessing which artefacts are required for a case, Axiom does provide assistance in that it assigns potential artefacts to categories such as “Chat”, “Cloud” and “Web Related”. But these are categories of the artefacts’ technical sources not how they can assist an investigation. For example, “Web Related” is a generic term and could encompass the URL of a visited site and also the volume name containing a viewed file. This broad, technical-based, categorisation still relies on an examiner knowing which artefacts may be present and how they may be compared.

Because there is no accurate description of the artefacts the examiner, to play safe, may select them all - this is not a scalable solution to the increasing volume of data.

6.6.2 Improving selection of artefacts using DESO

DESO is required to assess what system records on the computers may evidence the insertion of a USB device. To understand a method to exploit DESO, a short introduction to SPARQL [242] is required.

```
SELECT ?title
WHERE
{
<http://example.org/book/book1>
<http://purl.org/dc/elements/1.1/title>
?title .
}
```

Listing 6.1 SPARQL query to display any identified book titles

Introduction to SPARQL

DESO is an ontology specified as Resource Description Framework (RDF) [40]. This means it consists "subject, predicate, object" triples which are interpreted and linked together to form a conceptual model.

To query an RDF ontology, the most common method is to use the W3C standard: SPARQL Protocol And RDF Query Language (SPARQL) [242].

SPARQL queries operate by searching through the various triples for any that match a specified pattern. A simple query cited by W3C in its SPARQL specification is quoted as example.

Suppose an ontology is composed of the following Subject, Predicate Object triple:

<http://example.org/book/book1> (*subject*)
<http://purl.org/dc/elements/1.1/title> (*predicate*)
"SPARQL Tutorial" (*object*).

In other words, a book has the title "SPARQL Tutorial".

A sample of SPARQL code is shown at Listing 6.1. This reviews the available triples in the ontology for any matching this pattern. As follows:

- Variables are identified by a preceding "?" before the term;
- The "Select" clause directs which variable is to appear in any results; and
- The "Where" clause specifies the pattern that is to be used.

This pattern is run against the available triples and the corresponding variables are returned as results. In the stated example, the ontology's triples are reviewed for any that match the pattern where the *subject* is a book and the *predicate* is title. Where these occur, the *object* is returned. With the example, the result would be "SPARQL Tutorial".

This is a simple query but more complex ones can be formed. Results can be presented in a variety of formats. Further, queries on multiple ontologies can be performed at the same time - making SPARQL a powerful and efficient way of examining data held in an RDF format.

```
SELECT ?artefact ?type
WHERE
{
?type a deso:USB_Device_Identifier.
?artefact deso:isArtefactType ?type.
{?artefact rdf:type deso:OS_X_10.6.8}
UNION
{?artefact rdf:type deso:Windows_7}.
}
```

Listing 6.2 SPARQL query for any artefacts generated by OS X 10.6.8 or Windows 7 operating systems that are USB Device Type identifiers

To service these queries, local systems, such as Stardog [229], can be used to ingest the triple store and search them. Alternatively, SPARQL end points are available using HTTP to conduct queries over the internet.

Using SPARQL to query DESO for the selection of artefacts

Effectively, the examiner has to look for the potential links between either of the two computers and the USB stick - and focus in on these links, excluding the material which would not assist.

This requires the examiner to know what artefacts exist on the respective devices and, of those, which ones are potentially comparable. A commonly shared artefact, such as a serial number, allows this comparison. But there are others, and if the examiner is not aware of them, there is the possibility for missed opportunities to make connections in the data.

DESO has three strands: Location, Type Identifier and Reference. To use DESO for this enquiry, the Location strand has to be searched for any artefacts of the same Type Identifier present in both the USB stick and either the Windows PC or OS X machine Locations.

The first task is to catalogue the sources to understand their type of device, file system, operating system and any installed applications. Having completed this task, availability of artefacts is assessed - as discussed at Section 6.5.2. The available artefacts are then evaluated for any that share a common type between the USB device and either the Windows or OS X devices. Any artefacts of the same type can be compared.

An early approach to this scenario was detailed by Brady [35] as shown in the SPARQL code at Listing 6.2. However, there are limitations to this suggestion - illustrated at Figure 6.2.

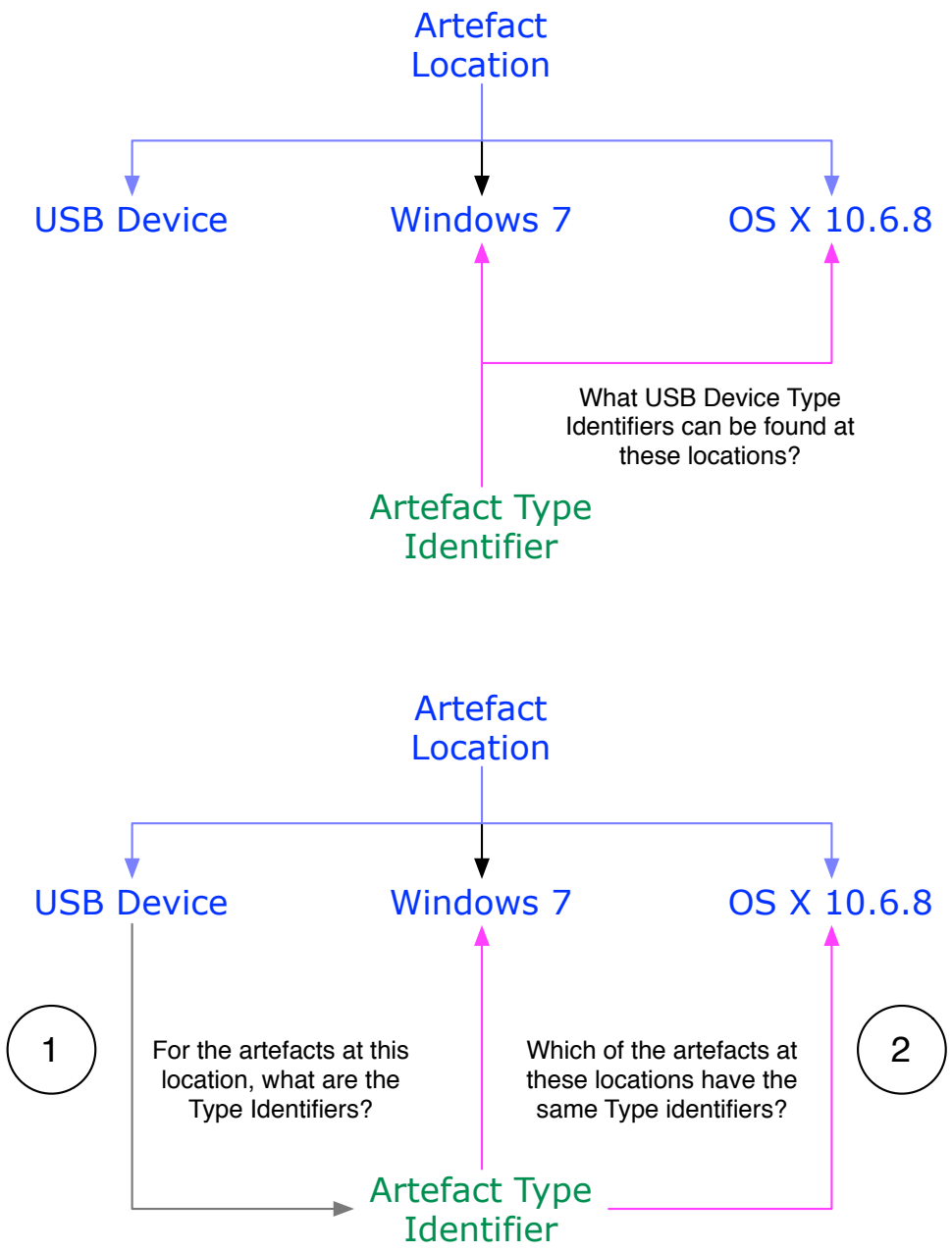

Fig. 6.2 Two approaches to searching for artefact Type Identifiers - the upper diagram illustrates an assumption that all USB Device Type Identifiers will be present on every USB Device. The lower diagram illustrates selection of suitable Type Identifiers on the Target only after those on the source have been identified.

Table 6.1

SPARQL Results: Artefacts found on a USB memory stick formatted with FAT32 that are also found on either Windows 7 or OS X 10.6.8

art 1	label 1	art 2	label 2	type
deso:Artfct 000014	USB Device Serial Number	deso:Artfct 000022	Windows 7 Software Registry EMDMgmt USB Serial Number	deso:Type 000011
deso:Artfct 000014	USB Device Serial Number	deso:Artfct 000023	OS X kernel USB Serial Number	deso:Type 000011
deso:Artfct 000020	Volume Serial Number	deso:Artfct 000031	Link File Volume Serial Number	deso:Type 000014

The upper diagram shows the original concept - the two computer locations were searched for the same Type Identifiers as should be found on a USB Device. The drawback to this approach is it assumes that all the artefacts located on any USB device have a Type Identifier from the USB Device sub-class. This may not always be the case. For example, in the future a USB Device may be developed with wireless networking capability. This would mean that it could generate artefacts with a Type Identifier from the "Network Address" sub-class.

To rectify this, the adopted approach is one illustrated by the lower diagram of Figure 6.2. The USB Device is first checked to establish what artefacts are available on it together with their Type Identifiers. The two computers are then checked for any artefacts with the same Type Identifiers.

A remedied SPARQL listing is shown at Listing 6.3. Also included in this code is an accommodation for any artefacts from the USB Device's file system, "FAT 32". Results from this query are shown at Table 6.1.

Displayed in this table are the pairs of artefacts from, respectively, the USB Device and either the Windows or OS X computers that match. Also shown is the common Type Identifier they share.

Note how one artefact from the USB Device, "deso:Artfct000014" can be compared to an artefact on each of the operating systems.

```
SELECT ?art1 ?label1 ?art2 ?label2 ?type
WHERE {

{?art1 rdf:type/rdfs:subClassOf* version15:USB_Device}
#Supplies all instances of selected class and sub-classes
UNION
{?art1 rdf:type/rdfs:subClassOf* version15:FAT32}.
#Supplies all instances of selected class and sub-classes

?art1 rdfs:label ?label1.
# Obtains label of selected instance

?art1 version15:isArtefactType ?type.
#Obtains DESO type of instance

{?art2 rdf:type/rdfs:subClassOf* version15:OS_X_10_6_8}
#Supplies all instances of selected class and sub-classes
UNION
{?art2 rdf:type/rdfs:subClassOf* version15:Windows_7}.
#Supplies all instances of selected class and sub-classes

?art2 version15:isArtefactType ?type.
# Compares Type of art1 against Type of art2

?art2 rdfs:label ?label2.
# Obtains label of selected instance

}
```

Listing 6.3 SPARQL query for any artefacts generated by USB Devices or FAT32 that shares a Type identifier with artefacts located on OS X 10.6.8 or Windows 7 operating systems.

Once DESO has been used to make this selection, tools - monolithic or open source - can be used to extract these artefact values and correlate them.

6.7 Testing the correlation of artefacts

It is assumed that the correct selection of artefacts has occurred and that the data values from these locations have been extracted. The task now is to compare these extracted values to understand if any found from the USB Device are also found on the computers.

6.7.1 The approach of monolithic tools

As a demonstration of the identified issues, the Axiom forensic tool ("Axiom Examine" version 1.0.5.1994") is again used as an example.

OS X operating system artefacts are not supported by Axiom so assessment concentrated on intra-Windows and USB device capability and the format Axiom used to export this data. This is so that the data could be compared to the output of other tools.

Axiom does aggregate various data sources - for example its "USB Devices" tab draws together data from various areas such as the Windows device installation log file and registry to provide examiners with a single view of a device's serial number, name and volume serial number.

However as with all the three tools tested, Axiom demonstrated a lack of internal consistency. As example, its "USB Device" and "Jump List" views are shown at, respectively, Figures 6.3 and 6.4.

Note the USB Device view shows the volume serial number represented in two formats - "VSN Decimal" and "VSN Hex". Yet in its "Jump Lists" view this same field is called "Volume Serial Number". Further, whether this field is displayed in decimal or hexadecimal is not specified.

If these Figures are inspected, it can be seen that the value "557180D" is displayed in the USB Device view. A similar value, "0557180D" is displayed in the Jump List view. It can surmised that this second notation is specified in hexadecimal but even this is shown with an additional "0" prefixed.

This creates problems when these values are exported and combined: what does a "VSN" or "Volume Serial Number" represent and in what format is it presented?

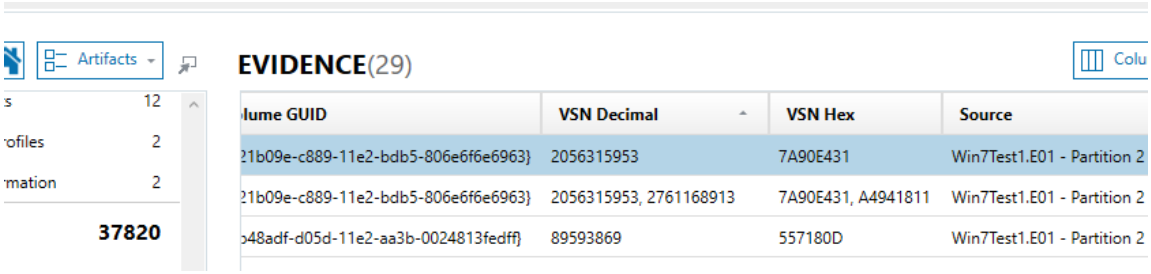

Fig. 6.3 Axiom's USB Device view describing the Volume Serial Number as "VSN" in both hexadecimal and decimal formats. Note the value "557180D" for reference when viewing Figure 6.4

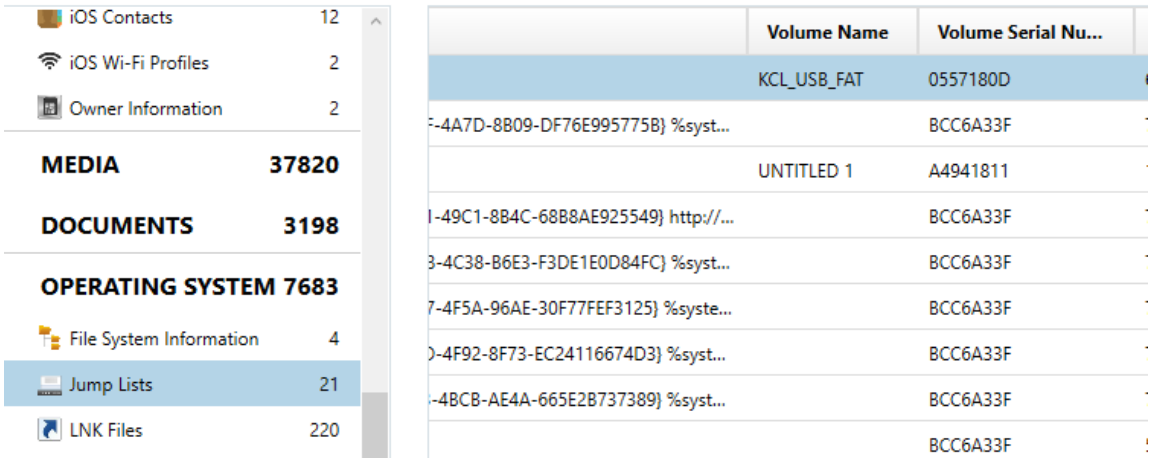

Fig. 6.4 How Axiom displays the parsed Volume Serial Number data from a Windows 7 Jump List. Note how it is not now described as "VSN" and the format is unspecified. Also note how the value "557180D" from Figure 6.3 is now listed as "0557180D"

As earlier reported, since Axiom does not parse OS X operating system artefacts, for effective use its output must be compared with that produced by tools that can parse this data. Figure 6.5 illustrates the issues when this occurs. The output from Axiom is combined with that from Encase version 7.10. Of note:

- Both tools use a field descriptor such as "Serial Number" without specifying to what this "Serial Number" relates? Without this clarification two, completely unrelated serial numbers could be compared.
- Field descriptors are not consistent within the tool - see Encase's "Serial #" and "Serial Number"
- Field descriptors are not consistent between tools - see Encase's "Volume Serial" and Axiom's "VSN Decimal"
- Data is reported differently by the tools - both data that each tool has extracted from the same apparent source - such as the "Last Connected" time - and data from disparate sources that are capable of comparison - such as "Serial Number".

In summarising the approach that Axiom and the other reviewed tools take, they rely on the examiner's historical knowledge or ability to research in order to understand how the various formats can be compared. In a simple USB stick scenario, this is entirely plausible but it may be less likely as more complex and obscure examination scenarios are encountered. The potential for errors and missed evidential opportunities exists.

6.7.2 Using DESO to aid correlation of heterogeneous sources

Instead of using proprietary descriptions, the various tools could report data using the DESO Artefact (Artfct) Number, Type Identifier and the data format dictated by the respective Type Identifier. Correlation within and between tools becomes possible. Figure 6.6 illustrates how this facility assists.

There are a number of points to draw out from this illustration:

- Those findings with the same Artfct number are from the same location - for example Artfct "0001". This means that different tools can be readily compared to understand if they are producing the same results.
- Those findings with the same Type Identifier number can be compared - eg Type "0002"
- The reported value is in a format dictated by the Type - this means that all tools report the data in the same way, no matter the source.

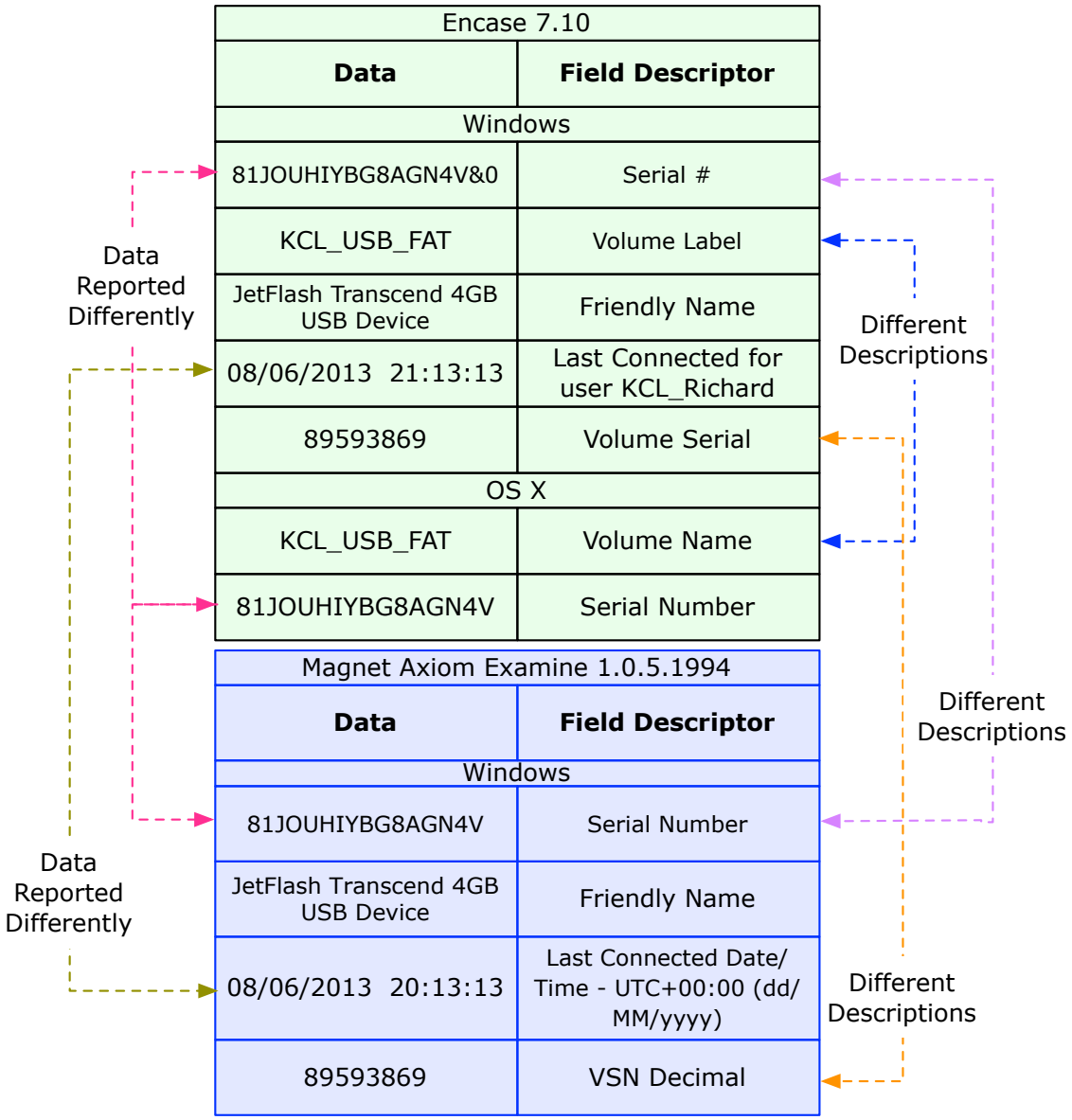

Fig. 6.5 An illustration of how artefact data, and they way this data is described, is reported differently both between tools and within the tool itself. This causes difficulties when comparison is made.

Encase 7.10				
Data	**Field Descriptor**	**DESO Artfct Number**	**DESO Type Number**	**Reported Value**
Windows				
81JOUHIYBG8AGN4V&0	Serial #	0001	0001	81JOUHIYBG8AGN4V
KCL_USB_FAT	Volume Label	0002	0002	KCL_USB_FAT
JetFlash Transcend 4GB USB Device	Friendly Name	0003	0003	JetFlash Transcend 4GB USB Device
08/06/2013 21:13:13	Last Connected for user KCL_Richard	0004	0004	08/06/2013 20:13:13
89593869	Volume Serial	0005	0005	557180D
OS X				
KCL_USB_FAT	Volume Name	0006	0002	KCL_USB_FAT
81JOUHIYBG8AGN4V	Serial Number	0007	0001	81JOUHIYBG8AGN4V

Magnet Axiom Examine 1.0.5.1994				
Data	**Field Descriptor**			
Windows				
81JOUHIYBG8AGN4V	Serial Number	0001	0001	81JOUHIYBG8AGN4V
JetFlash Transcend 4GB USB Device	Friendly Name	0003	0003	JetFlash Transcend 4GB USB Device
08/06/2013 20:13:13	Last Connected Date/ Time - UTC+00:00 (dd/ MM/yyyy)	0004	0004	08/06/2013 20:13:13
89593869	VSN Decimal	0005	0005	557180D

Fig. 6.6 Illustrates how DESO tags can be added to the output of monolithic tools. (Sample Artfct and Type Identifiers numbers used for illustration)

DESO is technology neutral - it is designed as a framework for capturing information about artefacts and providing for their accurate and consistent reporting. As such, no particular method for comparing artefacts is proposed. Possibilities include the use of spreadsheets and databases - or feeding the results into other ontologies. This may make for an interesting area of further research - discussed in Further Work at Chapter 8.

6.8 Assessing the reliability of artefacts

There are a number of occasions when the findings of an examiner need to be reported. These include:

- the preparation of a report detailing evidence for a judicial hearing - such as a criminal trial;
- the preparation of material for import into another analytical tool; and
- the preparation of material for transfer to another agency.

This can be time consuming - particularly where a large amount of artefacts require documentation.

6.8.1 The approach of monolithic tools

With regard to provenance, Axiom and the other tools tested do show the source of any reported artefact data. Examples are by reference to the location of the data in a file or, sometimes further, to a row number in the column of a database table. This is Level 1 Provenance as discussed earlier in Chapter 2 - see Table 2.1. This states how data can be located by others.

But there is no justification for any interpretation of these values. For example, the tool may assert that a particular value is a “Volume Serial Number” but does not state the reason for this assertion. This leaves the examiner having to trust that the developer of this product has made a correct judgement in its interpretation of the data at this location.

From an evidential standpoint, the examiner is left in a weak position without conducting further testing. But as the volume of artefacts in a case increases, this further testing may not be a practical expectation.

The examiner would, instead, be better served by the presentation of artefacts with greater evidence of provenance: at least Level 2, justifying the representation of this data as, for example, an IP address; but ideally Level 3 provenance would also be included which details what this data means - for example, the IP assigned to the device when connected to an internal network.

6.8.2 Using DESO to aid reporting of provenance

If the reporting format shown at Figure 6.7 is used, then the workload for the examiner is eased because evidence is produced as an automatic consequence of using DESO. Further, the provenance of the evidence is automatically documented.

If DESO is to have maximum utility, it cannot only document artefacts that have been tested and reported in peer reviewed journals. The field of digital evidence is advancing too quickly to be only captured by these information sources. Instead, sources such as blogs documenting artefacts must also be included.

But there is a difference in the reliability of the respective sources. An examiner has to assess this reliability when considering which artefacts to use and, further, what extra testing is required.

Using DESO, the examiner can review the information source for any artefact and easily note the provenance behind each one. This is performed using a combination of the source type and *hasProvenanceReference* object property.

For example, consider a DESO entry with only a blog entry for justification and the object property indicating that it is not peer reviewed and has no supporting material[1]. This may require further attention.

This ability to document and assess provenance may lend itself to analysis of evidential strength using probability measures. This is discussed in Chapter 8, Further Work.

With regard to the transfer of data to other agencies, particular those overseas, the reporting of DESO Artfct numbers and values may have particular utility. First, if other agencies also reference DESO, then there is no ambiguity surrounding the data being supplied. But second, it allows the transmission of disparate items of data without the need for surrounding context.

For example, network MAC addresses can be supplied for use in an overseas trial without the need to transfer a complete image of a computer. This may assist where there are data protection concerns for other data also contained on an evidence source.

6.9 Summary of assistance provided by DESO

In the previous sections, a number of problems were noted with monolithic tools:

1. The artefacts presented for the examiner's selection are based on the tool's capability - not the availability of artefacts. This means that potential artefacts are presented which, in fact, are not capable of being contained on the device. This also means that the examiner could miss potential artefacts if the tool does not support them.

2. The reporting and description of artefacts lacks precision and uniformity. This causes problems when comparing the outputs of disparate tools.

[1] hasProvCodeAuthStatNonPeerReviewedNotSupported

These problems can be addressed by buttressing them with DESO:

- instead of the tools being used to display and select artefacts, DESO is used and then the tools' capabilities are harnessed to perform this extraction;
- the tools use DESO to report their results - bringing benefits on comparability, reporting and provenance.

Figure 6.7 illustrates how DESO fits into the investigative workflow. Note how DESO does not aim to replace the tools - just aid selection of the correct one.

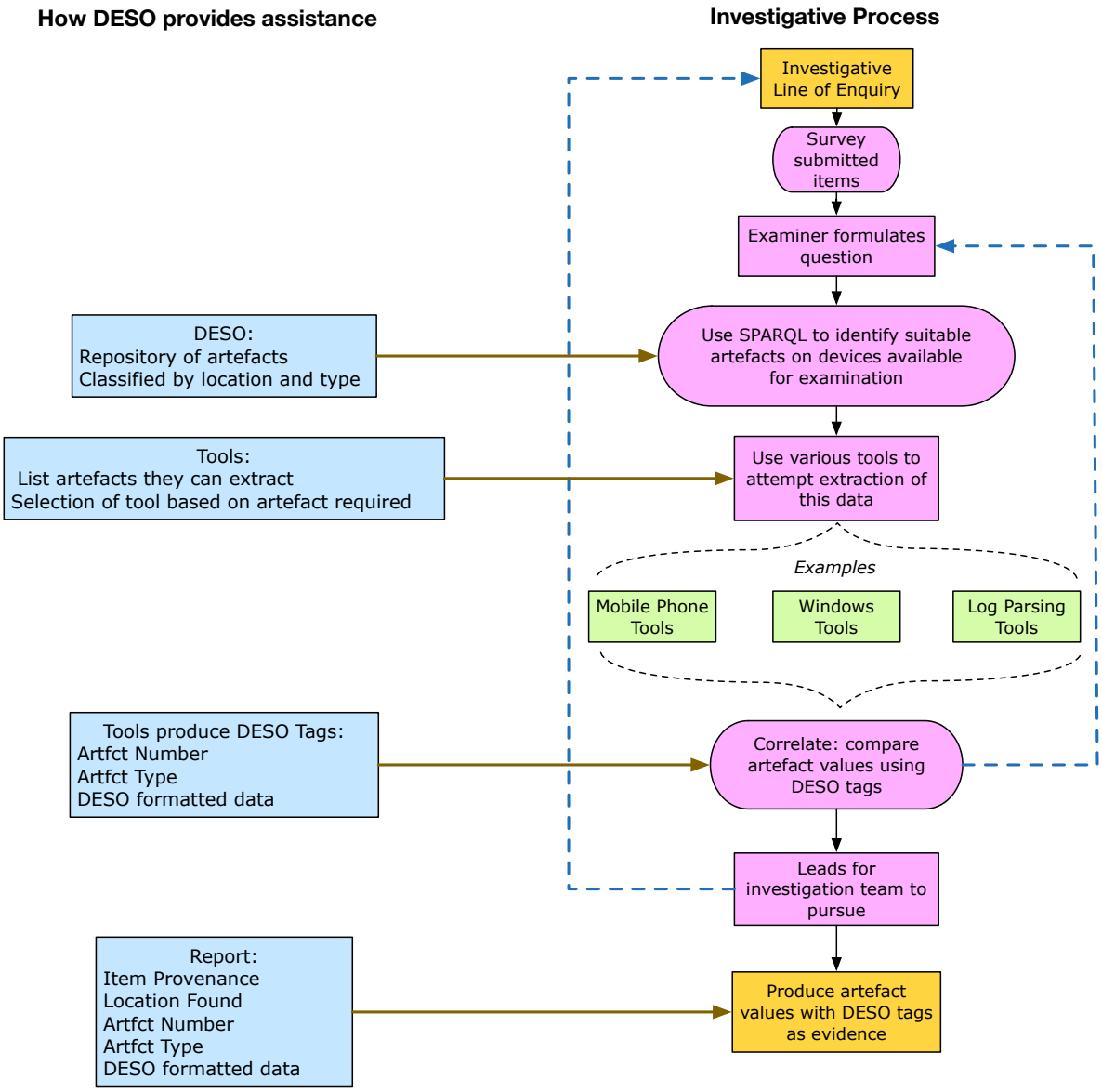

Fig. 6.7 DESO as part of the investigative process

To provide the greatest assistance to investigators, monolithic tools aim to cover as many data sources as possible. But there are deficiencies when the research problems of availability, selection, correlation and reliability are considered.

However, any issue taken with the tools is not the skill and effort that has been expended to produce them but the uses to which they are put. To expect one tool to perform every possible function is unrealistic - the use of these tools in this manner does them a disservice.

The situation is akin to using a large number of specially crafted scalpels to drill a specific hole from one side of a wall to the other. Each scalpel cuts material in a differing way to the others and may not even excavate in the required direction. If they are all used at the same time then, eventually, the hole will be cut but it may take longer than is required and the hole could be larger than is necessary.

But use of the correct scalpel at the correct time in the correct order completes the job faster and more efficiently. DESO performs this coordinating function.

Chapter 7

Evaluation of DESO against objectives

7.1 Introduction

The purpose of this chapter is to evaluate whether DESO addresses the thesis' Problem Statements.

The Problem Statements are set out in the Introduction at Section 1.2 but are repeated for ease of reference. The issue being addressed is development of a classification system to:

- Understand the available artefacts on any particular data source (Availability);
- Be able to select which of these artefacts are relevant to a particular enquiry (Selection);
- Provide a classification scheme to compare artefacts (Correlation); and
- Provide a mechanism for documenting the provenance of an artefact - the reason why a particular piece of data indicates a particular event (Reliability).

So DESO will be evaluated for Availability, Selection, Correlation and Reliability. In doing so, the Research Questions set out in Section 1.2 will be considered. These will be highlighted as they are encountered.

The evaluation addresses not just how DESO solves these issues but also how it does not. Recommendations for further work are made in Chapter 8.

In summing up, the principal Research Question will be considered: *Does DESO allow for the documentation of digital evidence artefacts and facilitates their extraction and comparison?*

7.2 Availability

Research Question 2: *Does DESO allow for differing digital sources and rapid changes in technology?*

This question primarily relates to the Location class. Chapter 6 demonstrated that DESO is capable of being populated with artefacts.

The Location class is extensible and the use of Uniform Resource Identifiers ("URI") [29] means that artefacts can be reorganised as required. This answers the Research Question.

For example, a global class for "IoT" devices may first be established but, as the field advances, this may require sub-division. As there is further maturity, there may no longer be a need for this "IoT" class at all.

But this organisation will require careful thought and consensus from the Digital Evidence community. This is essential to gain the support of those who could benefit from it - the ontological commitment described by Gruber [119].

Whilst fields such as fingerprints or ballistics show there are bodies that can reach such a consensus, as yet, no such international body in the digital evidence field has been identified that carries the authority to perform this task.

Aside from the Research Question, two other areas for consideration are DESO's remit and the way in which artefacts are placed within it. These will now be discussed.

7.2.1 The limited remit of DESO

Purposely, the scope of the artefacts captured in DESO is limited - it does not capture user data, general operating system data or digital evidence techniques - yet these could be of great benefit to an examiner.

The reason for this approach came from prior research. Technical information on various digital devices and systems was specified but the way in which this information could assist an investigation was often lacking.

DESO aims to address this point by linking all specified artefact Locations to a corresponding Type Identifier. If an artefact cannot be linked to a Type Identifier, it is not included. In this way an examiner is able to assess the availability of actual evidential artefacts, not just technical details.

At present, DESO's development has concentrated on documenting digital trace evidence between devices. This topic is again discussed in Further Work at Chapter 8.

7.2.2 The placement of artefacts in DESO

If DESO is to be effective, recording any artefact requires an instance to be placed in the correct Location sub-class. Otherwise, it will not be correctly identified as being available.

As an example of how this can go wrong, consider an artefact that is found in the Windows 7 Operating system. This needs to be represented in the DESO Location class. The relevant class structure is under “Operating Systems” where “Windows 7” could have two sub-classes underneath it representing “Service Pack 1” (SP1) and “Service Pack 2” (SP2).

The examiner wishing to find the correct Location sub-class in which to place the artefact works down through “Operating System” - as discussed at section 4.5.8. The “Windows” sub-class will be parsed followed by the one for “Windows 7”. Using the method currently defined, if the person creating this instance is unable to further identify whether the artefact is SP1 or SP2, the artefact is created in this, higher, Windows 7 Class.

But by creating the instance in this way, the examiner is implying that the artefact is present in all versions of Windows 7 - including both SP1 and SP2. This may not actually be the case, it is just the fact that the examiner has not been able to specifically identify the correct location for the artefact. There are two approaches to alleviate this problem.

The first is to create another ontology which details how the various classes such as Devices, File Systems and Operating Systems can be identified. This will include, for example, how to identify between Windows 7’s various Service Packs. This is discussed in Further Work, at Section 8.7. The purpose of this extra ontology is to assist any person to accurately identify the environment in which they have discovered an artefact.

A second approach is to carefully consider how the provenance of this artefact is recorded so that its reliability can be assessed. If the testing environment for this artefact has been adequately recorded then this should accurately state the equipment and operating systems used. From this, the “Service Pack” of the operating system should be apparent. If not then, when documenting the relationship between an instance in the Location class to its corresponding instance in the Reference class, the appropriate object property should be used. This can include:

- “hasProvCodeNoEvidenceAvailable” meaning that there is no evidence available to support this artefact; or
- “hasProvCodeAuthStatNonPeerReviewedNotSupported’ meaning that, although the, artefact has been documented, it is not supported by test data.

The conclusion to this debate is that great attention must be paid to the correct listing of classes and placement of artefacts. Whilst this may appear burdensome, any field involving classification has the same responsibility.

7.3 Selection

Research Question 3: *Can DESO reduce the volume of digital evidence that requires examination?*
Research Question 4: *Will DESO allow for the selection of artefacts based on investigative criteria as opposed to technical ones?*

The ability of DESO to answer these questions rests on the effectiveness of its "Type Identifier" class:

- DESO's largest class, "What", captures elements of trace evidence - showing how devices make records as they link together.
- The "Who" class documents where elements relating to identity are recorded and, by using the Friend Of A Friend ontology, uses a categorisation which can be readily interpreted by others.
- The "Where" class uses a number of other ontologies to categorise artefacts relating to geographical location.
- The "When" class has a measured application due to the the ambiguity of time when recorded by digital devices. It is a subservient class to the others instead of existing in its own right.

But conspicuous by their absence are the "How" and "Why' classes. By way of explanation, no one artefact in isolation was found to assist as an answer to these questions. Instead, multiple artefacts - by their presence or absence - may be required. This is an obvious deficiency when addressing Research Question 4. The topic will again be discussed later in Section 7.5 relating to Reliability and the requirement to define Level 3 Provenance - the meaning of an artefact.

Research Question 3 asked if DESO could reduce the volume of digital evidence that requires investigation. The answer to this question is a qualified yes.

DESO reduces the volume of digital evidence that requires examination because it can be used to select the required artefacts before data extraction takes place. This ensures that all the extracted data is relevant.

But one area where DESO may not be effective in reducing the volume of digital evidence is the examination of Operating System Independent files. This will be covered next.

7.3.1 The complication of Operating System Independent files

In assessing the utility of Type Identifier, further consideration is required when it is considered in conjunction with the Location Class for Operating System Independent Files

as detailed in section 4.5.5. This is due to the ubiquity and volume of these files on a device.

For instance, most devices will have large numbers of PDF or JPEG files contained at some position within their respective file systems. These can be system files of little immediate use to the investigation - such as icons and licensing agreements.

If, in the first instance, a device is parsed for these files, then there could be a large number of results. This does not assist with Research Question 3 dealing with volume.

An alternative approach would be to identify artefacts in the other Location sub-classes first and only consider Operating System Independent Files as a secondary approach if the first is unsuccessful.

7.4 Correlation

Research Question 5: *Can DESO allow for the successful comparison of artefacts irrespective of their source or originating format?*
Research Question 6: *Will DESO allow the use of any tools to process evidence?*

The use of a Type Identifier allows the identification of artefacts that can be compared with each other. Figure 6.6 demonstrated how the use of this Type Identifier provides a uniform format for reporting data values. This addresses Research Question 5. But there are situations where this approach will not be effective.

The first concerns data which is not adequately formatted. To illustrate this point, an example of data with a defined format is produced by the Institute of Electrical and Electronics Engineers (IEEE). This body specifies the format of an Ethernet addresses used for computer networking. This is typically in the form of numbers in hexadecimal interspersed by colons.

There may be variations to this format - for example some addresses may be stored without colons. But it should always be possible to transform the varieties into a uniform notation to allow comparison.

In contrast, examples of problem areas are user names and addresses. Although there are other external ontologies used by DESO, such as Friend Of A Friend [38], these allow the specification of a Type Identifier only. They are less stringent in specifying the format of data - for example, in an address, is “Road” always spelled this way or is it sometimes spelled as “Rd”?

The second concerns related but dissimilar data values. An example would be the correlation between GPS coordinates and, as used by the UK mail system, “Postcodes”. The reporting formats for these data can be specified in their respective Type Identifiers. But this does not assist in understanding that some of the reported GPS coordinates are contained within a particular Postcode area. So comparison could be made by translating these GPS coordinates into the relevant Postcode - or vice versa.

Both of these issues may be beyond the functional remit of DESO but there is contemporary discussion of them. The W3C has issued guidelines relating to best practice for publishing on the web generally [261] and, in particular, the use of spatial data [262]. One use of DESO may be as a component linking into the semantic referencing specified in these documents.

Research Question 6 asked if DESO could allow the use of any tools to process evidence. DESO does allow the use of any tools to process evidence because the reported artefacts are tool agnostic.

Indeed, if forensic tools listed the DESO artefacts they could extract it would provide for a more effective representation of a tool's capabilities. Further, this leads to a more accurate selection of a tool for a particular purpose.

7.5 Reliance

Research Question 7: *can DESO provide for the provenance of artefacts to be established?*

DESO is only partially successful in answering this question and further work is required.

To explain, when provenance was originally discussed, see Table 2.1, three levels were specified. DESO provides for Level 1 and Level 2 provenance. Level 1 is the actual Location of any data and, Level 2 is principally conveyed by its Type Identifier - what this data represents. And the reliability of the association between Location and Type Identifier is represented by the corresponding instance in the Reference class. The Object Property specifies the quality of this reference in supporting the association between Location and Type Identifier.

But the Type Identifier class does not necessarily provide assistance with Level 3 provenance: what does this artefact mean? For example, if the artefact is an IP address, what action or event does it represent? Is it the IP address of an external server or an address assigned to the computer on an internal network?

This debate is similar to earlier discussion of the How and Why Type Identifiers at Section 7.3. A possible explanation is there are few artefacts that, on their own, can justify a Level 3 interpretation. One artefact needs to be combined with others to form an evidence base before any such conclusion on meaning can be drawn.

There are two questions to ask in this respect: firstly, is it possible to specify a notation covering a number of artefacts that, by their presence and, possibly, absence, indicate a particular event? And, secondly, is DESO the correct mechanism to implement this notation?

With regard to the first question, it must be possible to draw conclusions about the meaning of one or more artefacts since this act is routinely performed for criminal proceedings involving digital evidence. An examiner would be reckless in presenting, for example, an IP address and then inviting the Court to speculate on what it means. Yet to guide any

Court on this meaning, the examiner must have conducted some sort of logical thought process. Indeed, during any trial, the examiner may be called upon to justify this process.

With regard to the second question, in its present form, DESO is not the right tool to provide Level 3 provenance. Instead, some sort of rule-based system could be developed which references both the presence and absence of particular DESO artefacts to suggest conclusions. This is addressed in Chapter 8, Further Work.

7.6 Summary

Research Question 1: *Does DESO allow for the documentation of digital evidence artefacts and facilitate their extraction and comparison?*

The evaluation of DESO has shown that the ontology is a good foundation for work in this field but not a complete one. Issues still to be resolved principally concern the complexity of situations - as seen in the "Why" and "How" categories and also the specification of Level 3 Provenance.

These, and other issues, are discussed in the next chapter, Further Work.

Chapter 8

Further work

The critical assessment of DESO in Chapter 7 identified that the class structure is a good foundation for the representation of Digital Evidence artefacts. However, this foundation has to be built up with further work. This is now detailed.

8.1 Type Identification classes - How and Why

Whilst Type Identification classes for What, Where, Who and When have been specified, How and Why remain. To cover these two, an idea is to join a number of artefacts together with extra property constraints.

In this sense they might form a series of lower level ontologies, perhaps using Expert Systems. These would use DESO as an upper level ontology for artefacts and their representation. The lower level ontologies could be environment specific because motivations and explanations may differ between the particular contexts they represent. Purely as an example, the use of encryption by a person with no other interest in technology might be more significant than when it is used by someone who routinely works in an IT-related environment.

8.2 Specification of artefact Location - a universal language

In section 4.5.3 the difficulty in specifying an artefact Location using a machine parsable format was noted. Suggestions included using Google's GRR language [58]. Further research into this field would be valuable because a notation system for artefacts would bring precision and, with increasing automation, an ability to code these locations for automatic extraction.

8.3 Modification of IoT and BAS systems for Digital Evidence

As discussed at section 3.4.4, the development of ontologies and classification systems for the Internet of Things (IoT) and Building Automation Systems (BAS) is more advanced and consensual than noted for the Digital Evidence field. And now the potential for forensic evidence from these devices is being discussed [93, pg 9], [184] [222].

This is fertile area for further research because of the changing use of technology. Desktop and laptop computers may no longer be the primary source of evidence - instead, as well as mobile devices, it is the circumstantial evidence created by IoT devices and BAS that may come to the fore. And, as shown, such ontologies are already developed and could be integrated into DESO.

8.4 Provenance ratings to assess weight of evidence

Section 5.2.2 discussed how the provenance of an artefact could be assessed by understanding the source of the information behind any assertion - its origin and relevance to the artefact being described. For instance, there is a difference between an artefact detailed in a web blog with no evidence of testing and one from a referenced and peer-reviewed journal with published test data.

An interesting area for further research would be to consider how these provenance ratings could be combined into a knowledge based system informing a collection strategy - as suggested by Keppens et al [153].

An implementation could look at the available artefacts but its selection of those to extract is guided not just by investigative objectives but, also, the reference source behind each artefact. For example, if there was a choice between an artefact that was well documented and tested and one which was not, it would be prudent to choose the former. This saves the examiner's time as less work would have to be performed testing any results.

8.5 DESO reporting to aid tool testing

A benefit of defined artefacts and uniform reporting is in the testing of tools. This is because the tool is used to extract data from a specific DESO Location and report it in the format specified by the Type Identifier.

As such, testing can be largely automated by running sample data with known results through the software and checking that the pre-determined DESO artefacts have been correctly located and displayed.

Benefits arising from this are:

- software developers will find it easier to test new versions of software because, after each iteration of development, it can be checked to ensure that it still performs the DESO artefact extractions accurately; and
- examiners can perform "calibration" testing on new tools to ensure that the artefact is extracted as claimed.

This may lend itself to some sort of certification scheme and so assist the presentation and acceptance of Digital Evidence in criminal trials.

8.6 Fragments of data

Examiners may find fragments of data that are not directly attributable to a particular file. This is particularly the case when conducting keyword searches across areas that are not allocated to any extant file: "unallocated". In this space there may be pieces of files that have been previously deleted.

The problem is to understand the file to which the data relates and its significance to enquiries.

But if certain data structures within the file can be identified - such as a particular file header or a prefix - then DESO's Data Properties, detailed in Section 4.5.3, can be used.

The data structures can be compared to the Data Properties listed in DESO for any that match. The artefacts that have these particular properties could then be further investigated to understand if they are the source of the fragment.

Interestingly, if DESO is sufficiently well populated, then it could be used to show only a particular artefact has the identified data property. It acts as an evidence base to rule out other possibilities.

8.7 Expanding DESO's coverage

In Section 7.2.1 it was noted how DESO was limited to actual evidential artefacts and did not cover, for example, Digital Evidence techniques. This is an area that could be expanded. The benefit of using an ontology for DESO is that the terminology in it can also be used in other ontologies - linking the two.

For example, if an ontology of techniques was developed, this could be cross-referenced to DESO artefacts so that an examiner could readily understand not just the artefacts that existed but also how to extract them.

Similarly, an ontology of tools could be developed and cross-referenced to the DESO artefacts that each tool could successfully extract.

As noted at Section 7.2.2, a useful addition would be an ontology specifying the identifying markers for various devices, operating systems and files. This could then feed

into DESO's Location class and aid more accurate identification and placement of artefacts within this structure.

8.8 Use of the dateAddedToDESO data property

In a conventional investigation, the envisaged enquiries would take place soon after the suspected offence. But this is not always the case. Other enquiries may take place some time later - particularly for "Cold Case Reviews" - the fresh examination of a previously unsolved case.

A key aspect of these enquiries is the use of analytical techniques - such as DNA examination - that were not available, or unknown, to the original investigation team. This could also occur with Digital Evidence.

For example, a mobile phone handset may have security features that make examination impossible at the time of the original investigation. But by the time of the Cold Case Review, flaws subsequently found in this mobile phone's implementation of security could allow access to the artefacts it contains.

In such circumstances, DESO can be searched for any artefacts with a "dateAdded-ToDESO" that is subsequent to the original investigation. This checks whether there are potentially useful artefacts available for examination that have subsequently come to light.

Chapter 9

Summary and conclusions

9.1 Summary of work

In Chapter 2 the basic concepts of criminal investigation are introduced. These included the Who, What, When, Where, How and Why questions that are framed to according to the various Lines of Enquiry. These "5WH" questions are later used in the Type Identifier class in DESO.

Contemporary areas of forensic evidence examination involving fingerprints, ballistics and DNA are discussed at section 2.4. The conclusion reached is that the construction and use of standards is a strong element of these disciplines. But also, that the construction of these standards relied on central bodies - often part of or related to a government - for their formation. DESO's evaluation in Chapter 7 also noted that a similar body may be required for Digital Evidence.

After a general introduction to Digital Evidence, its use in criminal investigations is introduced at section 2.8. The four Problem Statements are set out. That is to: understand the available artefacts on a particular digital evidence source; be able to select those which are relevant to an enquiry, be able to compare artefacts; and be able to document the provenance of an artefact.

Two challenges facing the field are then discussed: volume and variety. The challenge of volume is to devise an examination method which makes the least investigative compromise and is sustainable. The challenge of variety exacerbates any inability to handle availability, selection and correlation.

A discussion of tools and approaches that may be able to assist with the Problem Statements is at Section 2.9. This is followed by a review of previous research on Digital Evidence and tools. The issues of availability, selection, correlation and reliance were continually discussed in this research. There were, however, few solutions proposed.

A review of modular and monolithic Digital Evidence tools concludes a lack of technical documentation hinders their assessment. The tools do not state which artefacts

they do and, equally importantly, do not cover so an examiner is not able to gauge their effectiveness.

To rectify this, a listing of artefacts is recommended so that a tool could explicitly state which of these it could extract. It also recommended that artefacts should be assigned a uniform type and format to aid correlation. Current efforts, such as the Cyber-investigation Analysis Standard Expression are noted as being a step in the right direction.

Chapter 3 introduces the concept of models - and, in particular, a specific subset called "ontologies".

A review of models addressing Digital Evidence found there were few that were anything other than meta-solutions. They advise on what a good solution should look like without actually proposing one.

In reviewing previous Digital Evidence ontologies, few attempts to model from the conceptual standpoint of an investigation were noted. Instead they chose to replicate technical data in an ontological structure.

Chapters 4 and 5 introduce the Digital Evidence Semantic Ontology (DESO). The ontology consists three classes covering, respectively: the locations that artefacts can be found, the type of data at these locations and the reference sources behind these assertions.

The Location class is structured in such a way that it can be modified to take into account the constantly morphing technological fields. It was demonstrated how DESO's class structure can take changes into account whilst still retaining backwards compatibility. This is achieved through the use of Uniform resource Identifiers (URIs).

The placement of artefacts is discussed at section 4.5.8 and a method is proposed for deciding where an artefact should be positioned in the Location Class structure. This method also demonstrates how any search could be subsequently conducted.

To assist selection and correlation, every artefact recorded in the Location class must have a corresponding entry in the Type Identifier class. This is detailed in Chapter 5. In this way, all artefacts are meaningful - rather than just being data.

Fundamental to the Type Identifier Class is the use of the immediate sub-classes Who, What, When, Where, How and Why (5WH). These guide the examiner along investigative lines when considering the types of evidence to select for extraction.

Chapter 5 also highlights, at section 5.1.5, how the same data can have multiple uses and how some of these uses may not be immediately apparent to an examiner.

The Reference class relates to provenance Levels 2 and 3 - see section 2.9.1. This is not the physical location of data but how this data can be represented and also its meaning. A class system is set up to represent the various reference sources reinforced by object properties from artefacts in the Location class. The object properties indicate the type of provenance provided by the reference. In so doing they allow an examiner, or others reviewing the evidence, to understand the foundations upon which it is built. This aids assessment of reliability.

Later review of this class shows that, whilst it is competent in addressing Level 2, further work is required when considering Level 3 provenance.

Chapter 6 tests DESO by addressing a simple scenario - understanding the links formed when a USB memory stick is inserted into two desktop computers. Monolithic tools are used to address particular investigative processes. DESO is then implemented to understand how it can assist these tools.

In an evaluation at Chapter 7, DESO is found to assist in understanding which artefacts are available and, then, which are necessary to achieve the investigative objective. In doing so, the various digital evidence tools are used for extraction of data not as complete solutions.

Chapter 8 takes DESO's evaluation forward by suggesting new areas for further work. Ideas include: grouping sets of artefacts to form How and Why Type Identifiers; and a method for using the provenance rating from the Reference Class to inform the selection of artefacts.

9.2 Conclusions

This thesis argues that an ontology can:

- allow an examiner to understand the available artefacts on any particular digital evidence source;
- allow an examiner to select from the available artefacts based on the needs of particular enquiry;
- allow an examiner to compare artefacts; and
- assist an examiner by documenting the provenance of an artefact so that its relaibility can be assessed.

DESO has been shown to successfully address these challenges, although it is accepted that the research marks a starting point and not a final solution.

The overall insight is that the field of Digital Evidence is short of a controlled vocabulary to record and discuss artefacts. Until such time as one is formed, the effectiveness of any Digital Evidence tools will be severely hampered because they are limited both in their accuracy and, also, their ability to share and correlate results.

The contributions of the research will first be discussed followed by the identified limitations of the work and lessons learned.

9.3 Contributions of the research

9.3.1 Controlled vocabulary for recording artefacts

One of the key contributions of DESO is that it provides a controlled structure and vocabulary for the recording of Digital Evidence artefacts.

When other artefact recording systems were reviewed, they either lacked this structure and vocabulary or concentrate on recording artefacts after they have already been extracted.

The described utility of DESO comes from the use of an ontology. The structure of its Location class avoids ambiguity when considering an artefact's source and, as will be later described, is also extensible to cope with changes in technology.

The use of a controlled vocabulary is crucial because it provides a common means of communication - allowing the findings from different examiners and tools to be combined and compared. It also brings a precision where, previously, terms were ambiguous.

For example, a piece of data listed as a "Created Date" may be put forward as, for example, the date that a file was first stored on a device. But DESO, by its specification of both the location of this artefact, and also documenting the evidence behind it, works to ensure that all those using this data are able to assess its reliability.

One issue arising from the implementation of DESO is that it may highlight the paucity of research behind artefacts currently put forward as evidence.

9.3.2 Extensibility / adaptability

Key to DESO's utility is the adaptability provided by the use of URIs for instances - ie the artefacts - and the use of an ontology formed of Triples. As shown in Sections 4.5.2 and 4.5.2, this means that classes can be rearranged, refined and expanded as technology changes.

To illustrate this point, consider the artefacts listed in repositories such as the Artifact Genome Project - described in section 2.9.8. The location of the artefacts it documents are "hard-coded" - ie the full path is explicitly stated. But this does not lend itself to flexibility if there are any changes.

For example, if an artefact is listed as being found in the future operating system "Windows 11", this may be coded as such. But how will this be represented if a Service Pack of Windows 11 is introduced and, with its implementation, the artefact is no longer found in all subsequent versions of the operating system?

In contrast, as discussed at section 4.5.2, with DESO the class structure can be remodelled to represent the addition of a Service Pack. The position of the artefact can then be changed to reflect that it is only found in versions of the operating system before this Service Pack was introduced.

The contribution of this feature is that DESO can tolerate the changing nature of technology - both in the actual technology itself and also the types of artefacts that are to

be found on it. This assists in allowing an examiner to understand the available artefacts on any given Digital Evidence source.

9.3.3 Organised on investigation lines

A further contribution of DESO is the ability to organise and search artefacts from an investigative perspective.

It has been shown how existing artefact records and monolithic tools represent sources of Digital Evidence from a purely technical perspective. They offer selections on the source of the evidence, such as Internet History, rather than the contribution that this source can make to an investigation.

The danger of this approach is that it relies on the skill, knowledge and experience of the examiner. The technical sources have to be transformed to satisfy the investigative lines of enquiry. Using the example of Internet History, consider an examiner who is tasked with establishing whether a suspect viewed a particular document. For an effective enquiry, the examiner has to know that, as well as containing a list of websites visited, the Internet History can include a record of files viewed and the names of the volumes upon which they were contained.

If the examiner is not fully aware of this, then potentially useful evidence can be missed. As variety increases, so does this danger.

DESO's Type Identifier Class aims to alleviate this danger. It breaks down these technical sources into the evidential artefacts they provide - categorising them along the investigative Who, What, Where, When, How and Why lines of enquiry.

This is achieved by ensuring that, for every artefact listed in the Location class, it has an object property pointing to an entry in the Type Identifier Class. An artefact cannot be completed without entries in Location, Type Identifier and Reference classes. This ensure that DESO is a collection of useful artefacts rather than just a list of technical data.

If this is followed through to the Internet History, the artefacts could include a destination search on Google Maps in the internet history (Where), the time of this search (When) and the volume name of a file subsequently opened on a storage device (What). This not only gives a much richer picture of the data but it is also efficient - only the data relevant to the enquiry is extracted.

This contributes a solution for the Selection problem because an examiner will be able to search for the relevant 5WH sections of data across the whole range of devices being examined. This is an improvement on speculative review and a reliance on past experience.

It also reduces the volume of data that must be extracted to those items that are demonstrably relevant to the line of enquiry. This is in contrast to current approaches where data are first extracted and then, afterwards, reviewed for any relevance to the case.

9.3.4 Artefact placement and search

At section 4.5.8, a method was detailed for parsing DESO to initially place artefacts into an appropriate Location sub-class and then subsequently conduct searches. This involves methodically working down the appropriate Location class section until either the last identifiable class is found or, instead, the end of the class structure is reached.

Whilst limitations were identified with this approach - as detailed in the critical evaluation at section 7.2.2 - this is still a good starting point to launch further research. Current artefact repositories do not have a mechanism for searching. They are hampered by a lack of a controlled vocabulary which means that artefacts must be searched on, akin to, a keyword basis rather than a methodical approach.

9.3.5 Comparison of disparate sources

DESO not only provides a controlled vocabulary for documenting the Location that an artefact can be found, it also assigns a Type Identifier for the artefact that can be found at that location.

This assists an examination because it allows for the comparison of data which represent the same issue even though they are found in disparate sources. As example, a Media Access Control (MAC) address may be found on a mobile phone handset, wireless hot spot logs and mobile phone network records.

At present, there is no consistent terminology to unify these data for comparison. DESO allows this comparison to take place and ensures that all sources report using the same data format.

This approach also yields benefits when an examiner has one artefact of a specific type and wishes to find other artefacts of the same type which can be compared. DESO can be searched for this Type Identifier.

The contribution of this vocabulary is that it addresses availability, selection and correlation. An examiner no longer has to rely on their personal experience and recollection to understand the existence of artefacts and how they can be combined. Instead, this existence and utility is now documented.

The aggravating factor of volume is addressed because the examiner can hone in on the artefacts that are useful to the enquiry rather than collating large amounts of data. This means that searching through this data for patterns using keyword or “Big Data” techniques is not always necessary.

9.3.6 Mechanism for reporting and exchange of data

There has been no identified method for reporting digital evidence artefacts with precision. When either presenting to a judicial hearing - such as a criminal court - or disseminating intelligence to other parties, there is a difficulty in identifying the data that has been

extracted from a device and what it represents. DESO's contribution to this issue is two-fold.

First, in reporting evidential findings, data can be presented with the DESO artefact Location and Type Identifier. This saves the examiner's time.

It also means that any other examiner can locate this item of data from the same source without the requirement to use the same tool as the original examiner.

And, any other party can gauge the reliability of the findings by checking the Reference used to justify this artefact. There may be questions if an examiner is looking to put forward a case using artefacts for which no research has been conducted - purely relying on the stated output of a monolithic tool.

But second, this controlled vocabulary also contributes to the issue of data sharing. If the report from a monolithic tool is shared, the indistinct nature of the terms it contains can cause confusion.

Instead, if supplying the data together with the respective DESO Locations and Type Identifiers, then accuracy is improved.

9.3.7 Description of provenance

Whilst not an explicit research objective, the ability to describe the provenance of Digital Evidence has been a useful by-product.

Section 2.9.1 details how this provenance is described as three levels: the first relating to the location of the data itself, including any item's physical seizure and the position of the data within that device; the second is justification for the representation of the data - how, for example, a segment of binary can be represented as an IP address; and the third relates to the meaning of this data - for example, what does this IP address represent? Is it the last assigned external IP address when connected to a wireless router or the source IP address of a received email?

The description of these three levels provides a reference point for a debate on Digital Evidence. When evidence is presented to court, which of these levels is reached and by what means? Logically, all three should be fulfilled but, in delineating these separate requirements, proper consideration can be given to the issues and any identified gaps.

9.4 Identified limitations of the approach

9.4.1 Limited testing

DESO was developed organically with a number of prototypes discarded before a structure was found that fulfilled the objectives. Though this method of development is a form of continuous testing it has only had one person performing it. Further testing should involve the wider digital evidence community to ensure that it also understands the structure and use of the ontology.

The number of artefacts recorded in DESO has been purposely limited - so far only 31 instances. But with a settled structure, the population could increase to stress test DESO and properly gauge its extensibility.

In testing the application of DESO, this has also been limited to its use with monolithic tools. This was chosen because of the potential benefit to the field - monolithic tools are still widely used. But further testing should include the application of DESO to an actual criminal case, either past or present. The difficulties in conducting this testing are acknowledged - particularly with regard to disclosure issues - but this approach could be a useful way to prove DESO's value - or otherwise.

9.4.2 Outstanding issues

Whilst DESO has fulfilled the objectives, there are still outstanding issues to be resolved before more detailed testing takes place. These are principally outlined in chapter 8, Further Work. They include:

- A notation system for precisely articulating the position of artefacts in a machine-readable form; and
- The specification of How and Why Type Identifiers and queries.

9.4.3 Criteria for success

The success of DESO will principally depend on exponents in the Digital Evidence field submitting artefacts for inclusion. For this to happen, there has to be a belief that the ontology is worthwhile and has the support of the community - effectively, ontological commitment. When other forensic evidence fields are reviewed, some sort of national or international intervention is required to attain critical mass for these classification systems. At the moment, it is not possible to state which body would take this task on.

Further, DESO will also require maintenance. The class system will have to be monitored and revised to take into account new locations and types of evidence. Again, other fields have required some sort of supervisory body to be responsible for this task.

Finally, examiners may need some sort of incentive to submit artefacts to DESO - for this requires effort and there must be a reason. But the submission and use of DESO artefacts could be a useful career boost for an examiner - and those looking to enter the field such as students. The length of time taken to publish a paper in a peer-reviewed journal is too long to keep up with rapid technological changes. Inclusion of artefacts in DESO could be a faster route to recognition and use.

9.5 Lesson learned - the obscurity of ontologies

The use of ontological concepts when creating DESO has been valuable but has also caused a number of problems. The first is due to imprecise use of the term - which can mean anything from a short statement of concept to a large complex model. This can lead to difficulties in communicating what is being referenced.

The second is that, whilst well-known in the informatics arena, the term “ontology” is not known to many outside this circle. This presents difficulty in presenting DESO because an ontology must be explained before DESO’s function is conveyed. The obscurity of the term could also lead to some resistance in encouraging take up.

Whilst the use of an ontology would still be recommended for future work, it may be better not to use the actual word - instead calling it a “model” or “classification”. This may make the material more accessible.

References

[1] Access Data (2017). Forensic toolkit (ftk). http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk. (Accessed on 09/04/2017).

[2] ADF Solutions (2017a). Adf - home. http://www.adfsolutions.com/. (Accessed on 07/04/2017).

[3] ADF Solutions (2017b). Technical specifications. http://www.adfsolutions.com/docs/TechnicalSpecifications.pdf. (Accessed on 26/05/2017).

[4] Agarwal, R., Fernandez, D. G., Elsaleh, T., Gyrard, A., Lanza, J., Sanchez, L., Georgantas, N., and Issarny, V. (2016). Unified IoT ontology to enable interoperability and federation of testbeds. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, number i, pages 70–75. IEEE.

[5] Alink, W., Bhoedjang, R., Boncz, P., and Devries, A. (2006). XIRAF – XML-based indexing and querying for digital forensics. *Digital Investigation*, 3:50–58.

[6] Alzaabi, M., Jones, A., and Martin, T. A. (2013). An Ontology-Based Forensic Analysis Tool. In *ADFSL Conference on Digital Forensics, Security and Law*, volume 1, pages 121–136.

[7] Alzaabi, M., Martin, T. A., Taha, K., and Jones, A. (2015). The use of ontologies in forencis analysis of smartphone content. *The Journal of Digital Forensics, Security and Law*, 10(4):105–114.

[8] Amato, F., Cozzolino, G., Mazzeo, A., and Mazzocca, N. (2017). Correlation of Digital Evidence in Forensic Investigation through Semantic Technologies. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 668–673. IEEE.

[9] American National Standard for Information Technology, Accredited Standards Committee INCITS (2008). At attachment 8 - ata/atapi command set (ata8-acs). http://www.t13.org/documents/UploadedDocuments/docs2008/D1699r6a-ATA8-ACS.pdf. (Accessed on 12/10/2016).

[10] American Natonal Standards Institute (1993). ANSI / NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information.

[11] Andrew, M. W. (2007). Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media. *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, pages 16–30.

[12] Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3):201–213.

[13] Aronson, J. D. (2008). Creating the Network and the Actors: The FBI's Role in the Standardization of Forensic DNA Profiling. *BioSocieties*, 3(2):195–215.

[14] Arquilla, J. and Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2):141–165.

[15] Artifact Genome Project (2017). Artifact genome project. https://agp.newhaven.edu/about/start/. (Accessed on 28/08/2017).

[16] Ashburner, M., Ball, C. A., Blake, J. A., Botstein, D., Butler, H., Cherry, J. M., Davis, A. P., Dolinski, K., Dwight, S. S., Eppig, J. T., Harris, M. A., Hill, D. P., Issel-Tarver, L., Kasarskis, A., Lewis, S., Matese, J. C., Richardson, J. E., Ringwald, M., Rubin, G. M., and Sherlock, G. (2000). Gene ontology: tool for the unification of biology. The Gene Ontology Consortium. *Nature genetics*, 25(1):25–9.

[17] Ayers, D. (2009). A second generation computer forensic analysis system. *Digital Investigation*, 6:34–42.

[18] Azfar, A., Choo, K.-K. R., and Liu, L. (2016). An Android Communication App Forensic Taxonomy. *Journal of Forensic Sciences*, 61(5):1337–1350.

[19] Balaji, B., Agarwal, Y., Berges, M., Culler, D., Gupta, R., Kjærgaard, M. B., Srivastava, M., Whitehouse, K., Bhattacharya, A., Fierro, G., Gao, J., Gluck, J., Hong, D., Johansen, A., Koh, J., and Ploennigs, J. (2016). Brick. In *Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments - BuildSys '16*, pages 41–50, New York, New York, USA. ACM Press.

[20] Barnum, S. and Griffith, R. (2017). Pull It Together: Enabling Interoperability of Digital Forensic Systems Using a Standard Representation and Supporting API. In *Digital Forensic Research Workshop*, Austin, Texas, USA.

[21] Baryamureeba, V. and Tushabe, F. (2004). The enhanced digital investigation process model. In *Proceedings of the Fourth Digital Forensic Research Workshop*, pages 1–9.

[22] BBC (2015). Sony pays up to $8m over employees' hacked data. http://www.bbc.co.uk/news/business-34589710. (Accessed on 03/06/2017).

[23] Beckett, J. and Slay, J. (2007). Digital Forensics: Validation and Verification in a Dynamic Work Environment. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 266a–266a. IEEE.

[24] Beebe, N. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. In *Advances in digital forensics V*, pages 17–36.

[25] Beebe, N. L. and Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2):147–167.

[26] Belkasoft (2017). Belkasoft evidence center 2017. https://belkasoft.com/ec. (Accessed on 05/08/2017).

[27] Ben-Kiki, O., Evans, C., and Dot Net, I. (2009). YAML Ain't Markup Language (YAML™) Version 1.2. http://www.yaml.org/spec/1.2/spec.pdf.

[28] Berners-Lee, T. (2006). Linked data - design issues. https://www.w3.org/DesignIssues/LinkedData.html. (Accessed on 21/03/2017).

[29] Berners-Lee, T. and Fielding, R. (2005). RFC3986 - Uniform Resource Identifier (URI). https://www.ietf.org/rfc/rfc3986.txt.

[30] Berumdez-Edo, M., Elsaleh, T., Branaghi, P., and Taylor, K. (2015). Iot-lite ontology. https://www.w3.org/Submission/iot-lite/. (Accessed on 29/05/2017).

[31] Bizer, C., Heath, T., and Berners-Lee, T. (2009). Linked Data - The Story So Far. *International Journal on Semantic Web and Information Systems*, 5(3):1–22.

[32] Boyd, C. and Forster, P. (2004). Time and date issues in forensic computing—a case study. *Digital Investigation*, 1(1):18–23.

[33] Bradley, J. R. and Garfinkel, S. L. (2015). Bulk Extractor 1.4 User Manual. http://digitalcorpora.org/downloads/bulk_extractor/BEUsersManual.pdf/.

[34] Brady, O., Overill, R., and Keppens, J. (2014). Addressing the Increasing Volume and Variety of Digital Evidence Using an Ontology. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 176–183. IEEE.

[35] Brady, O., Overill, R., and Keppens, J. (2015). DESO: Addressing volume and variety in large-scale criminal cases. *Digital Investigation*, 15:72–82.

[36] Brian Carrier (2005). *File system forensic analysis*. Addison Wesley Profssional.

[37] Brickley, D. (2016). Linked open vocabularies (lov). http://lov.okfn.org/dataset/lov/vocabs/foaf.

[38] Brickley, D. and Miller, L. (2014). Foaf vocabulary specification. http://xmlns.com/foaf/spec/. (Accessed on 21/01/2017).

[39] Brickley, D. and Miller, L. (2016). The FOAF Project. http://www.foaf-project.org.

[40] Brickley, D. and RV, G. (2014). RDF Schema 1.1. https://www.w3.org/TR/2014/REC-rdf-schema-20140225/. (Accessed on 09/05/2017).

[41] Brinson, A., Robinson, A., and Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*, 3:37–43.

[42] Broderick, S., Elm, D. L., Goldsmith, A., Haried, J., and Raj, K. (2015). Criminal E-Discovery - A Pocket Guide For Judges. http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/.

[43] Buchanan-Wollaston, J., Storer, T., and Glisson, W. (2013). Comparison of the Data Recovery Function of Forensic Tools. In *Advances in Digital Forensics IX SE - 22*, volume 410, pages 331–347.

[44] Bulbul, H. I., Yavuzcan, H. G., and Ozel, M. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, 233(1-3):244–256.

[45] Butler, J. (2010). *Fundamentals of forensic DNA typing*. Academic Press/Elsevier, Amsterdam Boston.

[46] Californian Association of Criminalists (2017). What is a Criminalist? http://www.cacnews.org/membership/criminalistics.shtml. (Accessed on 11/02/2017).

[47] Cambridge Dictionary (2017). artefact - meaning in the cambridge english dictionary. http://dictionary.cambridge.org/dictionary/english/artefact. (Accessed on 29/08/2017).

[48] Cambridge University Press (2017a). Cambridge English Dictionary. http://dictionary.cambridge.org/dictionary/english/model. (Accessed on 30/04/2017).

[49] Cambridge University Press (2017b). Taxonomy - Meaning in the Cambridge English Dictionary. http://dictionary.cambridge.org/dictionary/english/taxonomy. (Accessed on 30/04/2017).

[50] Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, 1(4):1–12.

[51] Carrier, B. and Spafford, E. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, 2(2):1–20.

[52] Carrier, B. D. (2006). *A Hypothesis-Based Approach to Digital Forensic Investigations*. Phd, Purdue University.

[53] Casey, E. (2010). Digital dust: Evidence in every nook and cranny. *Digital Investigation*, 6(3-4):93–94.

[54] Casey, E., editor (2011). *Digital Evidence and Computer Crime*. Elsevier Science.

[55] Casey, E. (2012). Editorial - Cutting the Gordian knot: Defining requirements for trustworthy tools. *Digital Investigation*, 8(3-4):145–146.

[56] Casey, E. (2016). Editorial – A sea change in digital forensics and incident response. *Digital Investigation*, 17:A1–A2.

[57] Casey, E., Back, G., and Barnum, S. (2015). Leveraging CybOX™ to standardize representation and exchange of digital forensic information. *Digital Investigation*, 12:S102–S110.

[58] Castle, G. (2014). GRR Artifacts. https://www.blackhat.com/docs/us-14/materials/us-14-Castle-GRR-Find-All-The-Badness-Collect-All-The-Things-WP.pdf.

[59] Cellebrite (2014). Cellebrite's Outlook For The Mobile Forensics Industry 2014. Technical report, Cellebrite.

[60] Chabot, Y., Bertaux, A., Nicolle, C., and Kechadi, M.-T. (2014). A complete formalized knowledge representation model for advanced digital forensics timeline analysis. *Digital Investigation*, 11:S95–S105.

[61] Chabot, Y., Bertaux, A., Nicolle, C., and Kechadi, T. (2015). An ontology-based approach for the reconstruction and analysis of digital incidents timelines. *Digital Investigation*, 15:83–100.

[62] Chandrasekaran, B., Josephson, J., and Benjamins, V. (1999). What are ontologies, and why do we need them? *IEEE Intelligent Systems*, 14(1):20–26.

[63] Charpenay, V., Kabisch, S., Anicic, D., and Kosch, H. (2015). An ontology design pattern for IoT device tagging systems. In *2015 5th International Conference on the Internet of Things (IOT)*, pages 138–145. IEEE.

[64] Chibucos, M. C., Siegele, D. A., Hu, J. C., and Giglio, M. (2017). The Evidence and Conclusion Ontology (ECO): Supporting GO Annotations. In *The Gene Ontology Handbook, Method in Molecular Biology*, volume 1446, pages 245–259.

[65] Chow, K., Law, F. Y., Kwan, M. Y., and Lai, P. K. (2007). The Rules of Time on NTFS File System. *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, pages 71–85.

[66] Chu, H.-C., Deng, D.-J., and Chao, H.-C. (2011). An Ontology-driven Model for Digital Forensics Investigations of Computer Incidents under the Ubiquitous Computing Environments. *Wireless Personal Communications*, 56(1):5–19.

[67] Clarke, S. (2009). *Good Practice and Advice Guide for Managers of e-Crime Investigations*. Association of Chief Police Officer of England, Wales and Northern Ireland.

[68] Clover, C. (2015). Chinese telecoms group's operating system targets internet connected devices. https://www.ft.com/content/240ef87e-fea8-11e4-8efb-00144feabdc0.

[69] Cohen, M., Bilby, D., and Caronni, G. (2011). Distributed forensics and incident response in the enterprise. *Digital Investigation*, 8(SUPPL.):S101–S110.

[70] College of Policing (2005). Practice advice on core investigative doctrine. Technical report, College of Policing, UK.

[71] Conlan, K., Baggili, I., and Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, 18(December 2015):S66–S75.

[72] Ćosić, J., Ćosić, Z., and Bača, M. (2011). An ontological approach to study and manage digital chain of custody of digital evidence. *Journal of Information and Organizational Sciences*, 35(1):1–13.

[73] Council of Europe (2001). European Treaty Series - Convention on Cybercrime. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[74] Cox, S. and Little, C. (2017). Time Ontology in OWL - W3C Working Draft 02 February 2017. https://www.w3.org/TR/owl-time/#time:Instant. (Accessed on 29/05/2017).

[75] Craiger, J. P. (2009). Digital Evidence Markup Language : An Object-Oriented , XML-based Model for Sharing Computer Crime-related Information. Technical report, (National Institution for Forensic Science, University of Central Florida).

[76] Cuzzocrea, A. and Pirrò, G. (2016). A semantic-web-technology-based framework for supporting knowledge-driven digital forensics. In *Proceedings of the 8th International Conference on Management of Digital EcoSystems - MEDES*, pages 58–66. ACM Press.

[77] CybOX (2017). Cybox - cyber observable expression. https://cyboxproject.github.io/. (Accessed on 29/08/2017).

[78] Dang, Q. H. (2015). Secure Hash Standard. Technical Report October, National Institute of Standards and Technology, Gaithersburg, MD.

[79] D'Arcus, B. and Glasson, F. (2009). The bibliographic ontology. http://www.bibliontology.com/. (Accessed on 22/01/2017).

[80] D'Arcus, B. and Glasson, F. (2016). Bibliographic ontology specification | the bibliographic ontology. http://bibliographic-ontology.org/. (Accessed on 13/05/2017).

[81] De Forest, P. (1999). Recapturing the essence of criminalistics. *Science & Justice*, 39(3):196–208.

[82] Department of Justice (DOJ) and Administrative Office of the U.S. Courts (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG) (2012). Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases. https://www.fd.org/sites/default/files/Litigation%20Support/final-esi-protocol.pdf.

[83] Dosis, S., Homem, I., and Popov, O. (2013). Semantic Representation and Integration of Digital Evidence. *Procedia Computer Science*, 22:1266–1275.

[84] Dossis, S. (2012). *Semantically-enabled Digital Investigations*. PhD thesis, Stockholm University.

[85] Drummond, N. (2016). The photography ontology. https://code.google.com/archive/p/photographyontology/downloads. (Accessed on 10/09/2016).

[86] Duke Law Center for Judicial Studies (2017a). Edrm model | edrm. http://www.edrm.net/frameworks-and-standards/edrm-model/. (Accessed on 25/03/2017).

[87] Duke Law Center for Judicial Studies (2017b). Edrm wall poster | edrm. http://www.edrm.net/frameworks-and-standards/edrm-model/edrm-wall-poster/. (Accessed on 25/03/2017).

[88] Duke Law Center for Judicial Studies (2017c). Xml 2.0 schema | edrm. http://www.edrm.net/frameworks-and-standards/edrm-xml/2-0-schema/. (Accessed on 25/03/2017).

[89] Edwards, S. (2016). The iOS of Sauron: How iOS Tracks Everything You Do. https://github.com/mac4n6/Presentations/blob/master/iOSofSauron-HowiOSTracksEverythingYouDo/iOS_of_Sauron_04162016.pdf.

[90] Egas, M., Dieckmann, U., and Sabelis, M. W. (2004). Evolution Restricts the Coexistence of Specialists and Generalists: The Role of Trade-off Structure. *The American Naturalist*, 163(4):518–531.

[91] Elliott, J. (1997). *The Oxford paperback dictionary & thesaurus*. Oxford University Press, Oxford Tokyo.

[92] Encase (2017). Encase portable - triage & collect digital forensic evidence. https://www.guidancesoftware.com/encase-portable. (Accessed on 26/05/2017).

[93] European Research Consortium for Informatics and Mathematics (2016). ERCIM News - Special Theme: Cyber Security. *ERCIM News - Special Theme: Cyber Security*, (106):64.

[94] Europol (2017). EU forensic experts call for action on new cyber investigation standard | europol. https://www.europol.europa.eu/newsroom/news/eu-forensic-experts-call-for-action-new-cyber-investigation-standard. (Accessed on 26/05/2017).

[95] Evidence and Ontology, C. (2017). Evidence & conclusion ontology - user guide. http://www.evidenceontology.org/userguide/#history. (Accessed on 27/05/2017).

[96] Facebook (2017). Facebook - log in or sign up. https://www.facebook.com. (Accessed on 01/01/2017).

[97] Farrell, G. (2015). Preventing phone theft and robbery: the need for government action and international coordination. *Crime Science*, 4(1):4.

[98] FIESTA project (2017). FIESTA-IOT - Federated Interoperable Semantic IoT Testbeds and Applications. http://fiesta-iot.eu/. (Accessed on 29/05/2017).

[99] Financial Serrvices Authority (2012). Conviction R v Ali Mustafa & ors, Southwark Crown Court.

[100] Fisher, B. A., Tilstone, W. J., and Woytowicz, C. (2009). *Introduction to criminalistics : the foundation of forensic science*. Elsevier Academic Press, Burlington, MA.

[101] Flandrin, F., Buchanan, P. W. J., Macfarlane, R., Ramsay, B., and Smales, A. (2014). Evaluating Digital Forensic Tools (DFTs). In *7th International Conference : Cybercrime Forensics Education & Training*, pages 1–16, Canterbury, UK.

[102] Frigg, R. and Hartman, S. (2017). *Models in Science*. Metaphysics Research Lab, Stanford University, Spring 2001 edition.

[103] Galton, F. (1892). *Finger Prints*. Macmillan and Co, London.

[104] Gandomi, A. and Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2):137–144.

[105] Garfinkel, S., Nelson, A., White, D., and Roussev, V. (2010). Using purpose-built functions and block hashes to enable small block and sub-file forensics. *Digital Investigation*, 7:S13–S23.

[106] Garfinkel, S. L. (2006). Forensic feature extraction and cross-drive analysis. *Digital Investigation*, 3:71–81.

[107] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7:S64–S73.

[108] Garfinkel, S. L. (2013). Digital media triage with bulk data analysis and bulk_extractor. *Computers & Security*, 32:56–72.

[109] Gaševic, D., Djuric, D., and Devedžic, V. (2009). Ontologies. In *Model Driven Engineering and Ontology Development*, pages 45–80. Springer Berlin Heidelberg, Berlin, Heidelberg.

[110] Gayed, T. F., Lounis, H., Bari, M., and Nicolas, R. (2013). Cyber Forensics : Representing and Managing Tangible Chain of Custody Using the Linked Data Principles. *COGNITIVE 2013 : The Fifth International Conference on Advanced Cognitive Technologies and Applications*, (c):87–96.

[111] Gene Ontology Consortium (2004). The Gene Ontology (GO) database and informatics resource. *Nucleic Acids Research*, 32(suppl_1):D258–D261.

[112] Gene Ontology Consortium (2014). The Evidence Code Ontology. http://www.geneontology.org/GO.evidence.shtml.

[113] Gill, P., Jeffreys, A. J., and Werrett, D. J. (1985). Forensic application of DNA "fingerprints". *Nature*, 318(6046):577–579.

[114] Golbeck, J. and Rothstein, M. (2008). Linking social networks on the web with FOAF: a semantic web case study. *Proceedings of the 23rd national conference on Artificial intelligence - Volume 2*, pages 1138–1143.

[115] Goldsmith, A. (2011). Introduction to the Environmental Crimes Issue of the USA Bulletin. *United States Attorneys' Bulletin*, 59(3):2–15.

[116] Gómez-Pérez, A., Fernandez-Lopez, M., and Corcho, O. (2004). *Ontological Engineering*. Advanced Information and Knowledge Processing. Springer-Verlag, London.

[117] Grossman, M. R. and Cormack, G. V. (2013). The Grossman-Cormack Glossary of Technology-Assisted Review. *Fed. Cts. L. Rev.*, 7(1):2.

[118] Gruber, T. R. (1993). A translation approach to portable ontology specifications. *Knowledge Acquisition*, 5(2):199–220.

[119] Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing? *International Journal of Human-Computer Studies*, 43(5-6):907–928.

[120] GSM Association (2013). Mobile Network Codes and Names Guidelines and Application Form. http://www.gsma.com/newsroom/wp-content/uploads/2013/10/TS.25-v1.0.pdf.

[121] GSMA (2017). GSM Association. https://www.gsma.com/. (Accessed on 17/09/2017).

[122] Gudjonsson, K. (2010). Mastering the Super Timeline With log2timeline. *SANS InfoSec Reading Room*.

[123] Guidance Software (2017a). EnCase Forensic Software - Top Digital Investigations Solution. https://www.guidancesoftware.com/encase-forensic. (Accessed on 07/04/2017).

[124] Guidance Software (2017b). Guidance software - endpoint data security, ediscovery, forensics. https://www.guidancesoftware.com/. (Accessed on 07/04/2017).

[125] Guo, Y., Slay, J., and Beckett, J. (2009). Validation and verification of computer forensic software tools—Searching Function. *Digital Investigation*, 6(SUPPL.):S12–S22.

[126] Hachem, S., Teixeira, T., and Issarny, V. (2011). Ontologies for the internet of things. In *Proceedings of the 8th Middleware Doctoral Symposium on - MDS '11*, number June 2009, pages 1–6, New York, New York, USA. ACM Press.

[127] Harichandran, V. S., Walnycky, D., Baggili, I., and Breitinger, F. (2016). CuFA: A more formal definition for digital forensic artifacts. *Digital Investigation*, 18:S125–S137.

[128] Harrill, D. and Mislan, R. (2007). A small scale digital device forensics ontology. *Small Scale Digital Device Forensics Journal*, 1(1):242.

[129] Heard, B. J. (2008). *Handbook of Firearms and Ballistics*. Wiley.

[130] Helano, J. and Nogueira, M. (2008). Ontology for Complex Mission Scenarios in Forensic Computing. *The International Journal of Forensic Computer Science*, 3(1):42–50.

[131] Hendler, J. (2001). Agents and the Semantic Web. *IEEE Intelligent Systems*, 16(2):30–37.

[132] Her Majesty's Inspectorate of Constabulary (2017). PEEL : Police effectiveness 2016, A national overview. https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/peel-police-effectiveness-2016.pdf.

[133] Herdale, G. (2015). Digital Investigation and Intelligence Policing capabilities for a digital age. http://www.npcc.police.uk/documents/reports/DigitalInvestigationandIntelligencePolicingcapabilitiesforadigitalageApril2015.pdf.

[134] Hobbs, J. R. and Pan, F. (2004). An ontology of time for the semantic web. *ACM Transactions on Asian Language Information Processing*, 3(1):66–85.

[135] Hoss, A. M. and Carver, D. L. (2009). Weaving ontologies to support digital forensic analysis. In *2009 IEEE International Conference on Intelligence and Security Informatics*, pages 203–205. IEEE.

[136] House of Commons Science and Technology Committee (2005). Forensic Science on Trial. Technical Report 7, House of Commons, UK, London.

[137] Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6):528–535.

[138] Hunton, P. (2010). Cyber Crime and Security: A New Model of Law Enforcement Investigation. *Policing*, pages 1–10.

[139] Hunton, P. (2011a). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, 7(3-4):105–113.

[140] Hunton, P. (2011b). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, 27(1):61–67.

[141] Inman, K. and Rudin, N. (2000). *Principles and Practice of Criminalistics*. CRC Press.

[142] International Telecommmunications Union (2010). E.164 The International Public Telecommunication Numbering Plan. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.164-201011-I!!PDF-E&type=items.

[143] Jacobs, E. (2017). Death of vine is a warning to social media stars and big brands. https://www.ft.com/content/61603872-b7c1-11e6-961e-a1acd97f622d. (Accessed on 21/01/2017).

[144] James, J. I. and Gladyshev, P. (2013). Challenges with Automation in Digital Forensic Investigations. http://arxiv.org/abs/1303.4498.

[145] Jeffreys, A. J., Wilson, V., and Thein, S. L. (1985). Individual-specific "fingerprints" of human DNA. *Nature*, 316(6023):76–79.

[146] Joint Working Group on Electronic Technology in the Criminal Justice System (2013). Best Practices for electronic Discovery in Criminal Cases. Technical report, Department of Justice and Administrative Office of U.S. Courts, Washington, US.

[147] Kahvedžić, D. and Kechadi, T. (2009). DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. *Digital Investigation*, 6:S23–S33.

[148] Kaneiwa, K., Iwazume, M., and Fukuda, K. (2007). An Upper Ontology for Event Classifications and Relations. In *AI 2007: Advances in Artificial Intelligence*, pages 394–403. Springer Berlin Heidelberg, Berlin, Heidelberg.

[149] Karie, N. M. and Venter, H. S. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, 60(4):885–893.

[150] Kean, T. H., Hamilton, L. H., Ben-Veniste, R., Fielding, F. F., Gorelick, J. S., Gorton, S., Kerrey, B., Lehman, J. F., Roemer, T. J., and Thompson, J. R. (2004). The 9/11 Comission Report. Technical report, National Commission on Terrorist Attacks Upon the United States.

[151] Keane, A. (2006). *The Modern Law of Evidence*. Oxford University Press.

[152] Kelly, G., Mastroeni, M., Conway, E., Monks, K., Truss, K., Flood, P., and Hannon, E. (2011). Combining diverse knowledge: knowledge workers' experience of specialist and generalist roles. *Personnel Review*, 40(5):607–624.

[153] Keppens, J., Shen, Q., and Price, C. (2010). Compositional Bayesian modelling for computation of evidence collection strategies. *Applied Intelligence*.

[154] Komarinski, P. (2005). *Automated fingerprint identification systems (AFIS*. Elsevier Academic, Amsterdam Boston.

[155] Laing, A. (2009). Dentist and son jailed for three years for insider trading. *The Daily Telegraph*. http://www.telegraph.co.uk/news/uknews/crime/6780821/Dentist-and-son-jailed-for-three-years-for-insider-trading.html.

[156] Lawton, D., Stacey, R., and Dodd, G. (2014). *eDiscovery in digital forensic investigations*. Home Office Centre for Applied and Strategic Research, London. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf.

[157] Lebo, T., Sahoo, S., and McGuiness, D. (2013). PROV-O: The PROV Ontology. https://www.w3.org/TR/prov-o/. (Accessed on 29/05/2017).

[158] Li Ding, Lina Zhou, Finin, T., and Joshi, A. (2005). *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, chapter How the Semantic Web is Being Used: An Analysis of FOAF Documents, pages 113c–113c. IEEE, Hawaii.

[159] Lillis, D., Becker, B., O'Sullivan, T., and Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, pages 9–20.

[160] Liu, J., Kammar, R., Sasaki, R., and Uehara, T. (2017). Malware Behavior Ontology for Digital Evidence. In *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 585–586. IEEE.

[161] Magnet Forensics (2017a). About the artifact exchange - magnet forensics inc. https://www.magnetforensics.com/artifactexchange/. (Accessed on 29/08/2017).

[162] Magnet Forensics (2017b). Magnet axiom. https://www.magnetforensics.com/magnet-axiom/. (Accessed on 10/06/2017).

[163] Mangold, K. C. (2016). Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

[164] Mashey, J. R. (1997). Big Data and the next wave of infraStress. *Computer Science Division Seminar, University of California, Berkeley*. http://static.usenix.org/event/usenix99/invited_talks/mashey.pdf.

[165] Metz, J. (2017). Artifacts definition format and style guide. https://github.com/ForensicArtifacts/artifacts/blob/master/docs/Artifacts%20definition%20format%20and%20style%20guide.asciidoc. (Accessed on 04/05/2017).

[166] Meyers, M. and Rogers, M. (2005). Digital Forensics: Meeting the Challenges of Scientific Evidence. In *Advances in Digital Forensics*, pages 43–50. Kluwer Academic Publishers, Boston.

[167] Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, 1(1):61–68.

[168] Mook, R. (2017). I ran Clinton's campaign, and I fear Russia is meddling with more than elections. https://www.theguardian.com/commentisfree/2017/feb/07/russia-hacked-us-election-democracy-vladimir-putin. (Accessed on 06/03/2017).

[169] Moreau, L., Groth, P., Cheney, J., Lebo, T., and Miles, S. (2015). The rationale of PROV. *Web Semantics: Science, Services and Agents on the World Wide Web*, 35:235–257.

[170] National Institute for Standards and Technology, US (2017). Minutiae interoperability exchange (minex) iii | nist. https://www.nist.gov/itl/iad/image-group/minutiae-interoperability-exchange-minex-iii. (Accessed on 18/02/2017).

[171] National Institute of Justice (2011). *The Fingerprint Sourcebook*. Dept. of Justice, Office of Justice Programs, National Institute of Justice. https://www.ncjrs.gov/pdffiles1/nij/225320.pdf.

[172] National Institute of Science and Technology (2017). National Software Reference Library. https://www.nsrl.nist.gov/. (Accessed on 25/03/2017).

[173] National Institute of Standards and Technology (2015). Computer Forensics Tool Testing Handbook. https://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf.

[174] National Institute of Standards and Technology (2016a). Mobile Device Tool Specification Version 2.0. https://www.cftt.nist.gov/documents/Mobile%20Device%20Tool%20Secification_v2.0.pdf.

[175] National Institute of Standards and Technology (2016b). Mobile Device Tool Test Assertions and Test Plan Version 2.0. https://www.cftt.nist.gov/documents/Mobile_Device_Tool_Test_Assertions_and_Test_Plan_v2.0.pdf.

[176] National Institute of Standards and Technology (2017). National Ballistics Toolmark Research Database. https://tsapps.nist.gov/NRBTD/Home/DataFormat. (Accessed on 19/02/2017).

[177] National Research Council of the National Academies (2009). *Strengthening Forensic Science in the United States: A Path Forward*. National Academies Press, Washington, D.C.

[178] Nelson, A. (2012). *Advances in Digital Forensics VIII*, chapter XML Conversion of the Windows Registry for Forensic Processing and Distribution, pages 51–65. Springer, Pretoria, South Africa.

[179] Nimbalkar, P., Mulwad, V., Puranik, N., Joshi, A., and Finin, T. (2016). Semantic Interpretation of Structured Log Files. In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, pages 549–555. IEEE. http://ieeexplore.ieee.org/document/7785790/.

[180] Noy, N. F. and McGuinness, D. L. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Stanford Knowledge Systems Laboratory*, page 25. http://dx.doi.org/10.1016/j.artmed.2004.01.014.

[181] Nuix (2016). Nuix for Investigations. https://www.nuix.com/download/brochurenuixinvestigatorforlawenforcement. (Accessed on 09/04/2017).

[182] Nuix (2017). Class Hierarchy (scripting-api 7.0.2 API). http://developer.nuix.com/javadoc/ScriptingAPI/overview-tree.html. (Accessed on 09/04/2017).

[183] Ordnance Survey (2017). Postcode ontology. http://data.ordnancesurvey.co.uk/ontology/postcode/. (Accessed on 01/04/2017).

[184] Oriwoh, E., Jazani, D., Epiphaniou, G., and Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. In *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, number October 2013, pages 1–13. ICST.

[185] Oxford Dictionary (2017a). Definition of model in English. https://en.oxforddictionaries.com/definition/model. (Accessed on 30/04/2017).

[186] Oxford Dictionary (2017b). Definition of taxonomy in English. https://en.oxforddictionaries.com/definition/taxonomy. (Accessed on 30/04/2017).

[187] Oxford English Dictionary (2017). Definition of axiom in english by oxford dictionaries. https://en.oxforddictionaries.com/definition/axiom. (Accessed on 16/09/2017).

[188] Oxford Living Dictionaries (2017). artefact - definition of artefact in english | oxford dictionaries. https://en.oxforddictionaries.com/definition/artefact. (Accessed on 29/08/2017).

[189] Oxford Living Dictiony (2017). Definition of triage in english by oxford dictionaries. https://en.oxforddictionaries.com/definition/triage. (Accessed on 09/09/2017).

[190] Palmer, G. (2001). A road map for digital forensic research. In *First Digital Forensic Research Workshop, Utica, New York*.

[191] Pan, F. and Hobbs, J. R. (2004). Time in OWL-S. In *1st International Semantic Web Services Symposium*, pages 29–36.

[192] Park, H., Cho, S., and Kwon, H. (2009). Cyber Forensics Ontology for Cyber Criminal Investigation. *Forensics in Telecommunications, Information and Multimedia*, pages 160–165.

[193] Parsonage, H. (2009). Computer Forensics Case Assessment And Triage Discussion Paper. http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf. (Visited on 07/06/2014).

[194] Parsonage, H. (2010). The Meaning of Link Files in Forensic Examinations. http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf. (Accessed on 18/07/2017).

[195] Peroni, S. and Shotton, D. (2012). FaBiO and CiTO: Ontologies for describing bibliographic resources and citations. *Web Semantics: Science, Services and Agents on the World Wide Web*, 17:33–43.

[196] Pollitt, M. (2008). Applying Traditional Forensic Taxonomy to Digital Forensics. In *Advances in Digital Forensics IV*, volume 285, pages 17–26. Springer US, Boston, MA.

[197] Pollitt, M. M. (2007). An Ad Hoc Review of Digital Forensic Models. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, pages 43–54. IEEE.

[198] Pollitt, M. M. (2013). Triage: A practical solution or admission of failure. *Digital Investigation*, 10(2):87–88.

[199] Project Haystack (2017). Project haystack. http://project-haystack.org/. (Accessed on 30/05/2017).

[200] Quick, D. and Choo, K.-K. R. (2014). Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive. Technical Report 480, Australian Institute of Criminology. http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi480.pdf.

[201] Raghavan, S. (2012). Digital forensic research: current state of the art. *CSI Transactions on ICT*, 1(1):91–114.

[202] Raghavan, S. and Raghavan, S. V. (2010). Digital Evidence Composition in Fraud Detection. In *Digital Forensics and Cyber Crime*, pages 1–8.

[203] Raghavan, S. and Raghavan, S. V. (2013). A study of forensic analysis tools. In *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)*, pages 1–5. IEEE.

[204] Remus, D. A. (2014). The uncertain promise of predictive coding. *Iowa Law Review*, 99(4):1691–1724.

[205] Ribaux, O., Crispino, F., and Roux, C. (2015). Forensic intelligence: deregulation or return to the roots of forensic science? *Australian Journal of Forensic Sciences*, 47(1):61–71.

[206] Rivest, R. (1992). RFC 1321: The MD5 Message-Digest Algorithm. Technical Report April, MIT Laboratory for Computer Science. https://www.ietf.org/rfc/rfc1321.txt.

[207] Robertson, J. (2012). Forensic science, an enabler or dis-enabler for criminal investigation? *Australian Journal of Forensic Sciences*, 44(1):83–91.

[208] Rogers, M. (2004). The future of computer forensics: a needs analysis survey. *Computers & Security*, 23(1):12–16.

[209] Rogers, M. and Goldman, J. (2006). Computer forensics field triage process model. In *Conference on Digital Forensics, Security and Law*, pages 27–40.

[210] Rossy, Q. and Ribaux, O. (2014). A collaborative approach for incorporating forensic case data into crime investigation using criminal intelligence analysis and visualisation. *Science & justice: journal of the Forensic Science Society*, 54(2):146–53.

[211] Roussev, V. (2009). Hashing and Data Fingerprinting in Digital Forensics. *IEEE Security & Privacy Magazine*, 7(2):49–55.

[212] Roux, C., Crispino, F., and Ribaux, O. (2012). From Forensics to Forensic Science. *Current Issues in Criminal Justice*, 24(1):7–24.

[213] Roux, C., Talbot-Wright, B., Robertson, J., Crispino, F., and Ribaux, O. (2015). The end of the (forensic science) world as we know it? The example of trace evidence. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 370(1674):20140260.

[214] Ruibin, G., Yun, C. K., and Gaertner, M. (2005). Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. *International Journal of Digital Evidence Spring*, 4(1):1–13.

[215] Saad, S. and Traore, I. (2010). Method ontology for intelligent network forensics analysis. In *2010 Eighth International Conference on Privacy, Security and Trust*, pages 7–14. IEEE.

[216] Saleem, S. and Popov, O. (2013). Formal Approach for the Selection of a Right Tool for Mobile Device Forensics. In *5th International Conference on Digital Forensics & Cyber Crime*, Moscow.

[217] Schatz, B. (2007). *Digital evidence: representation and assurance*. Degree of Doctor of Philosophy, Queensland University of Technology. http://eprints.qut.edu.au/16507/.

[218] Schatz, B. and Clark, A. (2006). An open architecture for digital evidence integration. In *Proceedings of the 2006 AUSCERT R&D Stream*, pages 15–29. http://eprints.qut.edu.au/21119/.

[219] Schatz, B., Mohay, G., and Clark, a. (2006). A correlation method for establishing provenance of timestamps in digital evidence. *Digital Investigation*, 3:98–107.

[220] Schneider, P. (2013). DNA Databases. In *Encyclopedia of Forensic Sciences*, volume 1, pages 310–314. Elsevier.

[221] Schwartz, A. (2005). A Systemic Challenge to the Reliability and Admissibility of Firearms and Toolmark Identification. *Science and Technology Law Review*, 6:1–42.

[222] Serrano, M., Barnaghi, P., Carrez, F., Cousin, P., Vermesan, O., and Friess, P. (2015). Internet of Things - IoT Semantic Interoperability: research challeges, best practices, recommendations and next steps. Technical report, European Research Cluster on the Internet of Things.

[223] Shaw, A. and Browne, A. (2013). A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation*, 10(2):116–128.

[224] Shortall, A. and Azhar, M. A. H. B. (2015). Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. In Garain, U. and Shafait, F., editors, *2015 Sixth International Conference on Emerging Security Technologies (EST)*, volume 8915 of *Lecture Notes in Computer Science*, pages 188–199, Cham. IEEE.

[225] Slay, J. and Schulz, F. (2014). Development of an Ontology Based Forensic Search Mechanism: Proof of Concept. *Journal of Digital Forensics, Security and Law*, 1(1):25–44.

[226] Sleuthkit, T. (2017). Autopsy 3rd party modules - sleuthkitwiki. https://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules#Report_Modules. (Accessed on 06/04/2017).

[227] Smith, B. (2003). Ontology. In *Blackwell Guide to the Philosophy of Computing and Information*, pages 155–166. Blackwell, 2003 edition.

[228] Smith, D. C. and Petreski, S. (2010). A New Approach to Digital Forensic Methodology. In *Defcon 18*. https://www.defcon.org/images/defcon-18/dc-18-presentations/DSmith/DEFCON-18-Smith-SPM-Digital-Forensic-Methodlogy.pdf.

[229] Stardog (2017). Stardog: the Enterprise Knowledge Graph. http://www.stardog.com. (Accessed on 30/05/2017).

[230] Stephenson, P. (2002a). Analysis and Correlation. *Computer Fraud & Security*, 2002(12):16–18.

[231] Stephenson, P. (2002b). End-to-End Digital Forensics. *Computer Fraud & Security*, 2002(9):17–19.

[232] Stephenson, P. (2002c). The Forensic Investigation Steps. *Computer Fraud & Security*, 2002(10):17–19.

[233] Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report*, 8(2):42–54.

[234] Stevenson, A. and Soanes, C., editors (2008). *The Concise Oxford English Dictionary*. Oxford University Press.

[235] Stoll, C. (1990). *The cuckoo's egg : tracking a spy through the maze of computer espionage*. Pocket Books, New York. (ISBN 1416507787).

[236] Syed, Z., Padia, A., Finin, T., Mathews, L., and Joshi, A. (2016). UCO : A Unified Cybersecurity Ontology. In *AAAI Workshops*, pages 195–202.

[237] Technical Standardization Committee on AV and IT Storage Systems and Equipment (2012). *Exchangeable image file format for digital still cameras: Exif Version 2.3*. Japan Electronics and Information Technology Industries Association, Japan.

[238] The Forensic Wiki (2005). Revision history of "forensicswiki. http://forensicswiki.org/index.php?title=ForensicsWiki:About&action=history. (Accessed on 28/08/2017).

[239] The National Institute for Standards and Technology (2017). NIST Ballistics Toolmark Database. https://www.nist.gov/programs-projects/nist-ballistics-toolmark-database. (Accessed on 19/02/2017).

[240] The Sleuth Kit (2017). The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools. https://www.sleuthkit.org/index.php. (Accessed on 06/04/2017).

[241] The UCO Project (2017). Cellebrite case uco mapping. https://ucoproject.github.io/uco/mappings/Cellebrite-mapping.html. (Accessed on 13/09/2017).

[242] The W3C SPARQL Working Group (2013). SPARQL 1.1 Overview. https://www.w3.org/TR/sparql11-overview/. (Accessed on 09/05/2017).

[243] Thompson, R., Miller, J., Ols, M., and Budden, J. (2002). Ballistic Imaging and Comparison of Crime Gun Evidence - Appendix B. Technical report, US Bureau of Alcohol, Tobacco and Firearms. http://www.mcrkba.org/03-013_attach_B.pdf.

[244] Thompson, R. M. (2010). Firearm Identification in the Forensic Science Laboratory. Technical report, US National District Attorneys Association, Alexandria, VA, USA. https://www.nist.gov/sites/default/files/documents/forensics/Firearms_identity_NDAAsm.pdf.

[245] UK Government (1996). Criminal Procedure and Investigations Act 1996. http://www.legislation.gov.uk/ukpga/1996/25/section/23. Her Majesty's Stationary Office.

[246] UK House of Lords (1973). Dpp v kilbourne [1973] ac 729, 756, hl.

[247] US Supreme Court (1993). Daubert vs Merrell Dow Pharmaceuticals, Inc. 509:585–589. https://supreme.justia.com/cases/federal/us/509/579/case.html#opinion-pdf.

[248] USB Implementers Forum (2017). About usb-if. http://www.usb.org/about. (Accessed on 17/09/2017).

[249] Uschold, M. and Jasper, R. (1999). A Framework for Understanding and Classifying Ontology Applications. *Proceedings of the IJCAI-99 workshop on Ontologies and Problem-SolvingMethods (KRR5) Stockholm, Sweden*, 18:1–12.

[250] Valier, C. (1998). True Crime Stories - Scientific Methods of Criminal Investigation, Criminology and Historiography. *British Journal of Criminology*, 38(1):88–105.

[251] van Beek, H., van Eijk, E., van Baar, R., Ugen, M., Bodde, J., and Siemelink, A. (2015). Digital forensics as a service: Game on. *Digital Investigation*, 15:20–38.

[252] W3C Semantic Sensor Network Incubator Group (2011). Semantic Sensor Network Ontology. https://www.w3.org/2005/Incubator/ssn/ssnx/ssn. (Accessed on 29/05/2017).

[253] W3C Semantic Web Interest Group (2003). Rdf Vocabulary for Wgs84 Latitude/longitude/altitude Markup. Technical report. http://www.w3.org/2003/01/geo/wgs84_pos#.

[254] Walden, I. (2007). *Computer Crimes and Digital Investigations*. Oxford University Press.

[255] Walden, I. (2016). *Computer Crimes and Digital Investigations*. Oxford University Press. Second Edition.

[256] Wang, A. (2016). Can Alexa Help Solve a Murder? Police Think So - but Amazon Won't Give Up Her Data. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2016/12/28/can-alexa-help-solve-a-murder-police-think-so-but-amazon-wont-give-up-her-data/?utm_term=.b431c21f682d.

[257] Welch, C. H. (2006). Flexible Standards, Deferential View: Daubert's Legacy of Confusion. *Harvard journal of law & public policy*, 29(3):1085–1105.

[258] Whitcomb, C. M. (2002). A historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, 1(1):No longer in print.

[259] Willassen, S. Y. (2008). *Methods for Enhancement of Timestamp Evidence in Digital Investigations*. PhD thesis, Norwegian University of Science and Technology.

[260] Wilsdom, T. and Slay, J. (2006). Validation of Forensic Computing Software Utilizing Black Box Testing Techniques. In *Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December*, page 10.

[261] World Wide Web Consortium (W3C) (2017a). Data on the Web Best Practices. https://www.w3.org/TR/dwbp/#provenance. (Accessed on 01/07/2017).

[262] World Wide Web Consortium (W3C) (2017b). Spatial Data on the Web Best Practices. https://www.w3.org/TR/sdw-bp/. (Accessed on 01/07/2017).

[263] Wright, J. (2003). Detecting Wireless LAN MAC Address Spoofing. https://www.helpnetsecurity.com/dl/articles/wlan-mac-spoof.pdf.

[264] WTNH News 8 (2017). University of new haven launches artifact genome project - wtnh connecticut news. http://wtnh.com/2017/08/21/university-of-new-haven-launches-artifact-genome-project/. (Accessed on 29/08/2017).

Appendix A

Generation of test data

1. Windows 7 and OS X 10.6.8 operating systems were installed on hard disks using default settings. All media had been previously wiped using Encase version 6.19. A USB drive was formatted using the FAT 32 file system.
2. Sample files were copied on to the USB drive which was then inserted into both the Windows and OS X machines and those files accessed.
3. Both computers were then re-imaged

Appendix B

Table detailing Digital Evidence ontologies

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Ontology for Digital Evidence Bags [218] 2006	Ontology: the recording of meta-data regarding digital evidence storage formats. Builds a standard terminology for representing meta-data concerning integrity and provenance as well as the file content itself.	Concept	Yes	Not generally. But may be of use for RQ3 to document extracts of data from sources - ie rather than extracting all of the data from a device, just extract the small, relevant portion and use the ontology to document it.
Cyber Forensics Ontology [41] 2006	Ontology: Describes the cyber forensics domain but specific concept is not clear. Stated aim is to assist with curriculum development. Includes sub-classes of 'Technology' and 'Profession' - one is mapped to the other. This assists in finding the correct layers for specialization, certification, and education within the cyber forensics domain	Concept	N/A	No
Upper Ontology for Event Classifications and Relations [148] 2007	Ontology: Classifies 'Events' - either natural or artificial - and the relationships between them. Uses this event ontology with sort-hierarchy in order-sorted logic. Marries these events to time and location.	Concept but fully developed with predicate logic to act as an upper level ontology.	Yes	Does not assist with availability and selection. May assist with correlation but insufficient detail to assess.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Forensics Ontology [217] 2007	Ontology: Represents Event Logs - as part of Forensics of Rich Events - and Provenance - in terms of processing. Uses two base classes: Entity and Event to represent tangible 'objects' and how they are changed in state over time. Uses three methods of interacting with event log based data: search, hypothetical entity correlation, and automated notification.	Concept	Yes - for event logs and other temporal and linear data sources.	Does not assist with availability and selection. Does provide a mechanism for correlation but insufficient detail to assess. The outlined "Events" may assist with reliance (RQ7) as they could show Level 3 provenance - the meaning of an artefact.
A Small Scale Digital Device Forensics ontology [128] 2007	Ontology: Small-scale digital devices No ontological structure is detailed.	A notional proposition - not fully developed as a concept.	No	No - even from the perspective of a taxonomy, the proposed ontology is not helpful as there is insufficient detail
Ontology for Complex Mission Scenarios in Forensic Computing [130] 2008	Ontology: Describes complex mission scenarios - those in which information changes continuously and quickly or scenarios requiring a large quantity of resource - such as personnel	Concept.	Not possible to assess from the detail supplied. The ontology just appears to be a formalisation of an organisation structure with no stated object or data properties.	Insufficient detail to assess.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Digital Evidence Markup Language [75] 2009	Ontology: Not called an ontology but has ontological purpose: to provide a standardized means of representing computer crime-related materials. Uses object oriented modelling to facilitate the sharing of digital evidence	Concept	As a mark-up language - yes.	This is a language for describing that artefact data that has been located so does not assist with availability and selection. Will not assist for correlation as there are no unifying terms to allow comparison of data.
Dialog - digital investigation ontology [147] 2009	Ontology: Four separate ontological concepts: Crime Case; Evidence Location; Information; and Forensic Resource. Only one section - the Windows registry is modelled in detail. This represents two classes - information and information location - then uses specific rules to draw inferences on those entries.	Concept - though a section on the Windows registry has been further detailed.	Not possible to assess - the related concepts are too high level. The classifications are very high level taxonomies with no stated data or object properties.	Its Evidence (later referenced as Information) Location ontology could be useful in modelling availability. Further, its system for tagging data could be useful for correlation but, for both, there is insufficient detail to further assess.
Cyber Forensics Ontology [192] 2009	Ontology - the broad arena of cyber crime Aims to build an ontology that can be applied to the data mining of cyber crime. Defines five broad areas that can capture the details of a case. Acts as a recording system.	Concept - details five main classes and one set of sub-classes. Does not details data or object properties.	Insufficient detail to assess.	No. Appears to be simply a database of crime investigation. Insufficient detail to assess with respect to the RQs. Perhaps could act as an upper level ontology.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Method Ontology for Intelligent Network Forensics Analysis [215] 2010	Ontology: the domain of network components and how attacks are launched on them. Uses classes for such topics as attack; attacker; system; and location. Links instances with properties such as causes; uses; or target.	Fully developed to classes and properties	Yes - in terms of modelling attacks. But this appears to a form of notation. It is unclear how the results would be used other than as a storage of knowledge from a particular incident. There is no standardisation of terms etc.	No - the ontology does not standardise the terms that are used so cross incident correlation could be problematic. If it was married with an upper level ontology then it could be of use.
An Ontology-driven Model for Digital Forensics Investigations of Computer Incidents under the Ubiquitous Computing Environments [66] 2011	Neither: no actual ontology or taxonomy specified.			No - insufficient detail to assess.
Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence [72] 2011	Taxonomy: covers the chain of evidence for digital evidence. Models the sources of digital evidence that may be collected; the actors who may handle it; and how they handle it.	Fully developed classes though object and data properties not observed.	Insufficient detail. This just documents the issue.	No - insufficient detail to assess.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
An Ontology-Based Forensic Analysis Tool [6] 2013	Ontology: The component and concepts of the smart phone environment. Provides a common terminology to allow queries across differing smart phone functions.	Concept - though there is brief mention of classes.	Yes - from a high level though more detail would be required for further assessment.	Yes - if the common terms of the smart phone environment were applied to other scenarios then this would assist with correlation (RQ5).
Semantic Representation and Integration of Digital Evidence [83] 2013	Ontology: a number of lightweight ontologies are proposed to aid semantic representation of heterogeneous data. Two are covered - one for storage media and the other for network traffic analysis.	Concept. Attempted to review full ontologies but they are no longer available at supplied link or on other open-source searching.	Yes - from a high level through more detail would be required for further assessment.	Possible assistance for selection, RQ3 as the ontology allows specific elements to be targeted instead of all data. But there is no assistance in how to choose an element. For correlation, no. It uses a number of small ontologies with no unifying abstraction layer.
Advanced time-line analysis model [60] 2014	Ontology: To represent subjects, actions and events for compilation into a time-line. Converts digital evidence artefacts into formalised set notation such that they can be represented in sequence.	Fully developed to classes and properties. Set notation used but stops short of defining boundaries on the members of a set.	Yes. Though critically relies on effective interpretation of timestamps - which is not detailed.	Yes - with conditions. Doesn't assist with availability and selection but could assist with correlation - providing a consistent format between various sources.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Ontology Based Forensic Search Mechanism [225] 2014	Taxonomy: To represent file types. Breaks down file types into music, video and images then further sub-classes for JPEG; PNG etc. Each sub-class is itself subdivided according to whether it is "suspicious".	Concept. Appears to be a bare taxonomy with one class and no object / data properties.	Yes - from a high level through more detail would be required for further assessment.	No. Insufficient detail to assess.
Ontology for the Representation of Digital Incidents and Investigations [61] 2015	Ontology: aims to be sufficiently complete and accurate to model any digital incident. Has three layers into which extracted "knowledge" is placed: Common; Specialised; and Traceability. The knowledge is, effectively, the results from various tools. These are then linked as events, subjects and objects.	Fully developed and tested.	Partially - although there may be shortcomings in its ability to model any digital incident. It is only set up to handle the output from a limited set of tools. There is no mechanism for correlating semantically equivalent data in different formats (unless this is the knowledge layers) and there is no mechanism for interpreting timestamps correctly. Bearing in mind that this ontology is aimed at presenting a timeline, this may be a problem.	Does not address availability and selection. May assist with correlation in the way that it forms a time-line from extracted data. However, no unifying terms specified for this to be effective.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
F-DOS [7] 2015	Ontology: to formally model the smart phone content for the purpose of forensic investigation Creates two layers: one as a mapping of the technical detail for a specific device which feeds into the other - an abstracted representation of data categories which is common across all devices.	Principally conceptual though some limited development of classes.	Yes - from a high level through more detail would be required for further assessment.	Insufficient detail to assess.
DFAX [57] 2015	Ontology: DFAX represents the procedural aspects of digital forensics. Models the evidence chain to assist the representation of provenance. Uses CybOX tags.	Goes beyond conceptual - partial development of classes and object properties. - but development has ceased.	Yes - from a high level through more detail would be required for further assessment.	It is a representational tool of what exists - not what can be found - so no assistance with availability and selection. Its representation of events using multiple artefacts could assist with RQ7 to document Level 3 provenance - the meaning of an artefact.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
Curated Forensic Artifact (CuFA) [127] 2016	Ontology: documents artefacts classified as being 'curated'. Ontological concept is not definitive - making assessment problematic. When an artefact is identified it is entered using three fields - Location; CuFA requirements; and Cybox object Type.	Concept - mentions Artifact Genome Project which is detailed in section 2.9.8.	Insufficient detail to assess. No actual typing of artefacts - just notation.	No. Impractical to assess due to lack of detail. Mechanism for joining disparate instances of same data not identified.
Semantic Interpretation of Structured Log Files [179] 2016	Taxonomy: structured representation of log files with unknown formats. Uses a number of modules: the first looks for columns in the data; the others are 'experts' for fields such as IP address, email, date / time etc that independently look at each column and assign it a ranking on how close it is to their respective formats. The 'expert' with the highest score is used to allocate the column to a UCO label - see below entry.	Concept. Only the column splitting module was reported as being tested.	Yes	Yes - assists with correlation (RQ4). Any encountered log files could be fed into the application and a knowledge base built up of the data to be found in them - this may assist with availability RQ1. One complication is interpretation - this method uses a low level data format and incorrect interpretation could lead to errors. Caution is required in assigning a semantic reference to these columns to avoid potential problems.

Name /Date	Description of Ontology and its application	Stage of Development	Effectiveness - Does the ontology address the purpose?	Does it Assist with the Research Questions (RQ)?
UCO: A Unified Cybersecurity Ontology [236] 2016	Ontology: focusses on the cyber security domain and provides a core cybersecurity ontology that facilitates data sharing across different formats and standards and allows reasoning to infer new information. Classes are purely focussed on network intrusion scenarios. Suggests how the ontology can be linked to other sources, such as dbpedia, to enrich knowledge.	Concept	Yes - with reservations. Although this is meant to be a high-level ontology there is, still, insufficient data to make a proper assessment. The last entry in Github for this project was from a high level and more detail would be required for further assessment.	Does not assist with availability or selection. For correlation in the network investigation arena, it should assist as it provides a unifying language for heterogeneous sources. But there is too little detail to assess.
Knowledge Driven Digital Forensics [76] 2016	Ontology: an architecture to enable forensic investigations. Uses four layers for knowledge, integration, reasoning and querying. Aims to extract output from various tools into a common format to allow querying.	Concept. Purpose of layers is stated but there is no detail of the mechanism by which any of the conversion can be achieved.	Insufficient detail to assess.	Does not assist with availability and selection - it relies on all the data first being extracted. If the concept was successfully implemented it would assist with correlation.
Malware Behavior Ontology for Digital Evidence [160] 2017	Ontology: To classify malware in such a way as it can be presented at a criminal trial	Five classes listed. Nothing else. No external listing	Insufficient detail to assess	Insufficient detail to assess.